NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SECURITY ISSUES AND RESULTING SECURITY POLICIES FOR MOBILE DEVICES

by

Jason L. Brooks and Jason A. Goss

March 2013

Thesis Advisor:	George Dinolt
Second Reader:	John Mildner

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 2013	Master's Thesis

4. TITLE AND SUBTITLE SECURITY ISSUES AND RESULTING SECURITY POLICIES FOR MOBILE DEVICES	5. FUNDING NUMBERS
6. AUTHOR(S) Jason L. Brooks and Jason A. Goss	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ___N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	

13. ABSTRACT (maximum 200 words)

Mobile devices, given their promise of mobility with rich functionality, are being deployed with broadening use cases throughout the United States Department of Defense. All the while, massive quantities of information are stored and accessed by these devices without there being a comprehensive and specialized security policy dedicated to protecting that information. The importance of having a security policy grows as these devices start providing new capabilities and replacing many information systems we currently have deployed. Since the same device will be used in many different contexts, each with potentially different security policies, the devices will have to be able to adapt to those contexts. The security policy(ies) enforced by the device will have to adapt accordingly.

We investigate potential mobile computing security policies to balance this request for context aware functionality with the information assurance required of these government devices. We investigate the security issues raised in the use of these devices and provide example security policies that address some of these issues.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Cybersecurity, Mobile Devices, Mobile Phone, Context Aware Security Policy, Security policy, Mobile Security Policy	165
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 8–98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

SECURITY ISSUES AND RESULTING SECURITY POLICIES FOR MOBILE DEVICES

Jason L. Brooks
Civilian, Department of the Navy
B.S., University of South Carolina, 2000

Jason A. Goss
Civilian, Department of the Navy
B.S., East Stroudsburg University, 2006

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
March 2013

Authors: Jason L. Brooks and Jason A. Goss

Approved by: Dr. George Dinolt
Thesis Advisor

Mr. John Mildner
Second Reader

Peter J. Denning
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Mobile devices, given their promise of mobility with rich functionality, are being deployed with broadening use cases throughout the United States Department of Defense. All the while, massive quantities of information are stored and accessed by these devices without there being a comprehensive and specialized security policy dedicated to protecting that information. The importance of having a security policy grows as these devices start providing new capabilities and replacing many information systems we currently have deployed. Since the same device will be used in many different contexts, each with potentially different security policies, the devices will have to be able to adapt to those contexts. The security policy(ies) enforced by the device will have to adapt accordingly.

We investigate potential mobile computing security policies to balance this request for context aware functionality with the information assurance required of these government devices. We investigate the security issues raised in the use of these devices and provide example security policies that address some of these issues.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION AND BACKGROUND 1
A. THESIS STATEMENT AND MOTIVATIONS 1
B. THESIS SCOPE AND LAYOUT 2
C. WHAT IS A "MOBILE DEVICE" 2
D. MOBILE DEVICE USES IN THE DEPARTMENT OF DEFENSE 4
1. High-Level Functionality Requirements 6
2. Use Case Examples from Functional Objectives 11
3. Threats and Security Context of Mobile Device Use Cases 15
E. SUMMARY 21

II. SECURITY POLICY FOR MOBILE DEVICES 23
A. MOBILE DEVICES 23
1. Handheld Personal Computing Devices 23
a. Application Marketplace 25
b. Embedded and Expandable Sensors 26
2. Wearable Computing 26
3. Humanistic Intelligence–Embedded Technology 29
B. WHAT IS A "SECURITY POLICY" 30
1. Defining "Security Policy" 30
2. Information as the Transactional Entity 31
3. Security Objectives and Resources 33
4. Defining "Information Security Policy" 35
C. SECURITY POLICY DEVELOPMENT METHODOLOGY 38
1. Security Policy Levels and Examples 38
2. Engineering Process 45
D. DOD SECURITY POLICIES 51
1. Department of Defense (DoD) Security Policy 51
2. Executive, Federal, and Defense Organizational Policy 53
3. Security Controls 61
a. Family: Access Control (AC) [33] 62
b. Family: Audit and Accountability (AU) [33] 64
c. Family: Configuration Management (CM) [33] 67
d. Family: Incident Response (IR) 69
e. Family: Media Protection (MP) 70
f. Family: Identification and Authentication (IA) [33] ... 72
g. Family: System and Communication Protection Control (SC) [33] 74
h. Family: System and Information Integrity (SI) [33] ... 78
i. Family: Personnel Security (PS) [33] 81
j. Mobile Unique Security Controls: 82
4. System Specific Implementation 87

III. MOBILE DEVICE INFORMATION FLOW AND POLICY IMPLICATIONS... 91
A. SECURITY OBJECTIVES AND STATEMENT 91
B. CONCEPTS FOR IMPLMENTING MOBILE DEVICE SECURITY..... 93
C. APPROACHES TO MOBILE DEVICE INFORMATION FLOW ENFORCEMENT 96
1. Decentralized with Trusted User Conflict Resolution 97
a. Personality Information Flow Enforcement 98
b. Sensor Information Flow 102
c. Personality and Unified User Experience Information Flow 111
d. Analysis 113
2. Centralized 116
a. DoD Centralized Management 116

IV. CONCLUSION 119
A. SUMMARY 119
B. TOPICS FOR FUTURE RESEARCH 119
1. Declassifying, Sanitization, and Downgrading 119
2. Non-Persistent and Thin Personalities 120
3. Information Flow among Personalities, Sensors, Network Infrastructures, and Enclave 121
4. Information Flow among Personalities, Network Interfaces, and COI Infrastructures 122
5. Privacy and User Rights 123
6. Official Time Source among Personalities 123
7. Mobile Carrier Access to Device 124
8. Coordinating Classifications/Confidentiality Levels 124
9. Utilizing Context Awareness for Security 124
10. Security Services on Resource Limited Mobile Devices.. 126
11. High Availability Requirements 126
12. Choosing an Architecture for Mobile Devices with Personalities 127
13. Choosing and Applying a Formal Security Model for Mobile Devices 127
C. CONCLUSION 127
1. What is Unique about Mobile Devices 128
2. Security Implications 128
3. Proposed Approach 130
4. Analysis and Conflict Identification 131

LIST OF REFERENCES 133

INITIAL DISTRIBUTION LIST 143

LIST OF FIGURES

Figure 1. Example Notification from Google Glass. From [21] 27
Figure 2. Example Turn-by-Turn directions. From [23] 28
Figure 3. Information Security Policy Statement 37
Figure 4. Information Security Requirements Hiearchy 39
Figure 5. Information Security Construct 42
Figure 6. Example Information Security Construct Requirements Traceability .. 44
Figure 7. Engineering Process in the NIST RMF 46
Figure 8. SP 800–60 Security Categorization Process Execution. From [37] 48
Figure 9. Security Control Selection Process. From [13] 49
Figure 10. Checklist User Process Overview. From [36] 50
Figure 11. Multiple Personality Mobile Devices 93
Figure 12. Standard Notional Mobile Device Architecture After [74] 98
Figure 13. Personality Conflict Demonstration 100
Figure 14. Mobile Device Information Flow—Information Flow Block Request .. 106
Figure 15. Mobile Device Information Flow—Sensor Request 107
Figure 16. Trusted Application 113

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Purpose of a Security Policy 32
Table 2. NIST Security Controls. From [13] 40
Table 3. Military COI Sensor Policy (provided at personality load) 108
Table 4. Personal COI Sensor Policy (provided at personality load) 109
Table 5. Mobile Device Sensor Policy 109

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

APs	Access Points
ASD(NII)	Assistant Secretary of Defense for Networks & Information Integration
ASP	Automated Security Policies
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BYOD	Bring Your Own Device
CAC	Common Access Card
CD	Compact Disk
CDMA	Code Division Multiple Access
CEO	Chief Executive Officer
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CMST	The Centre of Microsystems Technology
CNSSAM	Committee on National Security Systems Advisory Memorandum
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COI	Community of Interest
COMSEC	Communications Security
CSS	Central Security Service
CUI	Controlled Unclassified Information
DAC	Discretionary Access Control
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoS	Denial of Service
DTM	Directive-Type Memorandum
DVD	Digital Video Disk

ECG	Electrocardiogram
EEPROM	Electrically Erasable Programmable Read-Only Memory
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standard
G&PM	Guidance & Policy Memorandum
GIG	Global Information Grid
GPS	Global Positioning System
HIPPA	Health Insurance Portability and Accountability Act
HPCD	Handheld Personal Computing Device
I&A	Identification and Authentication
IA	Information Assurance
IFB	Information Flow Block
IPS	Intrusion Prevention Systems
ISP	Internet Service Provider
JAG	Judge Advocate General
JBC-P	Joint Battle Command-Platform
JBC-P	Joint Battle Command-Platform
LCD	Liquid Crystal Display
MAC	Mandatory Access Control
MDM	Mobile Device Management
NACSI	National COMSEC Instruction
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security System
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OPSEC	Operations Security
OS	Operating System
OSP	Organization Security Policies
PII	Personally Identifiable Information
PKI	Public-Key Infrastructure

PTO	Personal Time Off
PYSOP	Psychological Operations
RATS	Raytheon’s Android Tactical System
RMF	Risk Management Framework
SCAP	Security Content Automation Protocol
SCIF	Sensitive Compartmented Information Facility
SCRM	Supply Chain Risk Management
SP	Special Publication
SRG	Security Recommendation Guides
SSI	System Specific Implementation
STIG	Security Technical Implementation Guide
U.S.	United States
USB	Universal Serial Bus
USGCB	United States Government Configuration Baseline
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Networks
WLAN	Wireless Local Area Network

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to first thank Jennifer Guild and the SPAWAR leadership, specifically our supervisors Dale Koeman and Damon Shivvers, who gave us this opportunity by bringing in the program and allowing us to make time for our classes.

We thank NPS, the support staff, and all our professors who suffered long VTC sessions in order to provide us with some much-appreciated education in the treacherous world of Information Security.

This thesis would not have been possible without the patience, guidance, and time from both our knowledgeable advisor and second reader, Dr. George Dinolt, and John Mildner. Their clear and entertaining explanations of complex topics made the development of this thesis enjoyable.

We could not have completed this thesis without the love, support, and encouragement of our families. Specifically, we would like to show our deepest gratitude to our wives (Amanda Goss and Kristina Brooks) for their unwavering support and sacrifices throughout our Master's program.

Finally, we would like to thank our parents who made us who we are, or ever hope to be. (Abraham Lincoln)

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION AND BACKGROUND

A. THESIS STATEMENT AND MOTIVATIONS

Since the announcement of the iPhone on 7 January 2007, a revolution has taken place in the mobile cell phone market that has changed phones into mobile computing devices. These devices are now being deployed into the battlefield and connecting to the Global Information Grid (GIG). In the commercial sector, corporations are now joining the Bring Your Own Device (BYOD) movement. All the while, massive quantities of information are stored and accessed by these devices without a comprehensive and specialized security policy dedicated to protecting it.

The Army has requested that the capabilities of these devices be delivered rapidly to the battlefield. Programs like Joint Battle Command-Platform (JBC-P) [1], Raytheon's Android Tactical System (RATS) [2] and Army Marketplace [3] are advancing the use of these handheld devices in the military to meet this demand. The United States Chief Information Officer (CIO) would like to start allowing these devices in the civilian government with the possible use of a public app store and secure private app stores in one device. The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) has already deployed 50 iPads, with interest in deploying 50 additional devices. Despite the desire to rapidly deploy these devices, little attention has been paid to their security and the secure integration of these devices into the GIG. The importance of a security policy grows as these devices start providing new capabilities and replacing many information systems we currently have deployed. Since these devices will be used in many different contexts each with potentially different security requirements, the devices will have to be able to adapt to those contexts. The security policy(ies) of the device will have to adapt accordingly.

We propose developing a mobile computing security policy to balance this request for functionality with the information assurance required of these

government devices. We provide examples of the security issues raised in the use of these devices and of potential policies that might be used.

B. THESIS SCOPE AND LAYOUT

This study applies to United States (U.S.) Government uses of mobile devices at the classified and unclassified levels for the full scope of Department of Defense (DoD) uses from the administrative to battlefield functions. In this thesis, we first attempt to define modern colloquial meaning of a mobile device, how they may be useful for DoD, and the reason a security policy is needed for these devices. Then, starting in Chapter II, we discuss the types of mobile devices and security policies as they relate to mobile devices by first describing what is a security policy, how to develop a security policy, what are the current DoD security policies. In Chapter III we suggest a future leaning approach to implementing mobile device security. Chapter IV will conclude with topics for future research and final thoughts on mobile device security.

C. WHAT IS A "MOBILE DEVICE"

Mobile computing devices or simply "mobile devices" for short come in many different forms, such as personal data assistants, smart phones, and tablets. Today, the most popular mobile devices are characterized by their size or "handheld" status, touch sensitive screens versus keyboards and mice, and wireless connectivity. They include devices commonly called "tablets" and devices doubling as cell phones, which are commonly called "smart phones." Mobile devices although very small and primarily used to consume digital content are also used to do many of the same things we expect from a traditional computer such as a desktop or laptop.

The National Institute of Standards and Technology (NIST) recently published their Special Publication 800–124 Revision 1 titled "Guidelines for Managing and Securing Mobile Devices in the Enterprise" [4] in which they define mobile devices as having the following characteristics:

- A small form factor
- At least one wireless network interface for Internet access (data communications). This interface uses Wi-Fi, cellular networking, or other technologies that connect the mobile device to network infrastructures with Internet connectivity.
- Local built-in (non-removable) data storage
- An operating system that is not a full-fledged desktop or laptop operating system
- Applications available through multiple methods (provided with the operating system, accessed through web browser, acquired and installed from third parties)
- Built-in features for synchronizing local data with a remote location (desktop or laptop computer, organization servers, telecommunications provider servers, other third party servers, etc.). [4]

The above is a good description of current mobile device technology. However, this paper considers a more expansive view of mobile devices and the future of mobile devices by choosing to focus on the "personnel" aspect of the device rather than the current capability and form. Another key aspect of these devices is how they serve as the catalyst for the fusion of information from multiple sources, at least from the owner's point of view, where there is a synergy provided to that user because all the information is presented in a consumable and personal fashion. Therefore, the device must be able to enforce the security policy as intended for each "flavor" of data handled on behalf of the user which is what makes the analysis of mobile device security policy more interesting and complex.

For the purposes of this paper, the term "mobile device" will mean a small and extremely light-weight personal computing device which uses as a primary

interface something other than the traditional keyboard, is connected via wireless technologies for data connection, is designed to operate predominantly on battery power, and is of a size and dimension such that it is easily transportable or wearable by a single person. Current examples of such devices are the iPhone, the iPad, Android OS phones, Android Tablets, Google Glass, and many other similar devices [5]. However, the future may bring wearable devices such as the new Google Glass, computers built into clothing, or any other conceivable device meant for personal data processing.

D. MOBILE DEVICE USES IN THE DEPARTMENT OF DEFENSE

A powerful and highly mobile computing platform, today's mobile devices offer a near desktop replacement in the palm of your hand. Mobile devices are so abundantly featured they offer solutions for many of today's information centric problems. From the dedicated executive to the soldier in the battlefield, these devices are highly sought after for the freedom they offer in terms mobile productivity [6], [7]. As a replacement to less mobile and less agile solutions, mobile devices are already being integrated into DoD operations. Mobile devices are being considered for several DoD projects. Some of these projects are: Air Force Judge Advocate General (JAG) replacement for Paper Documents; Air Force Electronic Flight Book for Aircraft Operations to replace heavy paper checklists and maps; Joint Battle Command-Platform (JBC-P); Raytheon's Android Tactical System (RATS); and the Army Marketplace.

This movement in the military is lagging behind the consumer marketplace. As of February 2012, 71 percent of U.S. adults in the 25 to 34 age bracket already own a Smartphone [8]. Along with these personal mobile devices, employers are also providing an additional mobile device. As a result, many professionals carry at least two mobile devices [8]. The juggling between these mobile solutions can cause professionals frustration, wishing for a simpler solution. This frustration along with the ability for "management to avoid upfront costs of mobile devices" [8] has led to the Bring Your Own Device

(BYOD) movement. With BYOD, employees bring their own mobile device for use by their employer. "This is already common in many businesses. In a 2012 Cisco survey performed in the U.S., 95 percent of respondents said that their organizations permit employee-owned devices in some way, shape, or form in the workplace" [8].

As this replacement and movement takes place, these mobile devices will dramatically increase the number of data owners accessing one device beyond currently deployed information systems. This issue is made additionally complex because mobile devices are highly available (always on), regularly reside on one's person (always on you), and often record and interpreting environmental data for context (contextually aware through sensors). These three conditions have increased the amount of information available to these devices. Additionally, these devices are used by individuals to fill information technology and communications needs across all the roles in their life. An example of such roles could include a DoD employee who is a father, volunteer firefighter, and active church member; or an accountant who is a son, military reservist, and woodsman. The user expects to use the mobile device to support these roles and all activities that accompany them. It is this combination of activities on one device with its combined information that raises information assurance considerations for both the employer's security and user's privacy. This thesis attempts to address these considerations through a security construct that would be enforced on these mobile devices.

In order to describe mobile devices and their corresponding security policy, we must first describe the environment for which mobile devices reside. To accomplish this we introduce the following terminology:

- ***Community of Interest (COI):*** Services provided by a community of information systems of like interest and/or purpose that operate with the same overall information protection needs.

- ***Personality:*** A label for information and applications on a mobile device that guarantees a given set of protection required by the related COI.

From the environmental definitions above, we propose that a mobile device consists of a single or multiple personalities defined by three values: COI, User, and physical mobile device. Personalities serve as a container or domain within the mobile device for information owned by the corresponding COI. COIs are a collection of service providers and the communications infrastructure corresponding to the capabilities and services offered to a user towards fulfilling a particular role within that community or organization. The COI communication infrastructure can vary greatly in a physical and virtual sense. A COI could consist of a set of applications, servers, or the entire communication infrastructure.

For mobile devices, commercial service providers, such as the Sprint, AT&T, or Verizon provide the vast majority of the COI communication infrastructure. However, there are multiple technical mechanisms to communicate with a COI. Wi-Fi would be an example of such a mechanism that could be provided publicly, personally, or directly by the COI. The battlefield would be a specific example of a COI providing the entire technical ability to communicate with that COI. In this example, the DoD implements GIG communication infrastructures that are specific to a single COI and may be completely physically or logically isolated from other communications infrastructures. Additionally, the segregation of COI communications infrastructure may be virtual, in the form of encrypted communications and virtual private networks (VPN).

1. High-Level Functionality Requirements

In order to define the security policy, high-level functional requirements must be clear for all information systems that communicate with the device. Since the functional requirements and security policies are already defined for

standard information systems, we have focused on functional requirements centered around mobile devices. Mobile devices can provide “unique” and “enhanced” functionality in comparison to the standard information systems currently used today. These two categories (unique and enhanced) are used for defining the combined high-level functional requirements for mobile devices. The first category of functionality is “unique” to mobile devices:

- ***Dynamic User-Centric Intelligence (DUCI)*****:** *Right information at the right time, as it relates to the user.* The mobile device is able to provide the information required based on an ecosystem that consists of the user’s role, information, and behavior, as well as the context of situation, and location. This information would automatically be provided when the ecosystem calls for it. Examples from above could include:
    - When a meeting is scheduled at a remote location, the traffic could be checked with the time of arrival calculated from your current position. An alert could then be sent to the user about when to leave. If the device notices that the user will be late, it could notify the person being met or even rebook flights.
    - When the user is interested in a specific topic or waiting on an announcement, the mobile device could notify the user of any changes in information. The mobile device could provide potential actions that can be taken from current location.
    - Military forces could be automatically notified of downed essential services or population unrest prior to entering an area with local populace.
    - Mobile devices that receive alerts on hostile forces, hazards, and roadblocks could automatically reroute the user around it using the navigational unit.

- ***On-Demand Agile Communication (ODAC):*** *Communicate continuously the way you want and when you want.* The mobile device should support a wide variety of communication options that are always available. These options should include support for communication across short and long distance. It should also support communications among devices when no external networks are available. The device should allow the user to choose the way that communication should occur. The device should also allow the user to provide information in the format that best fits the user's requirements, despite the communication path chosen. Examples from above could include:
    - Ammunition that is tracked by the mobile devices. These mobile devices could send alerts to command and logistics personnel when ammunition supplies are running low.
    - Military personnel could tag friendly and hostile forces in an augmented reality from their headgear or weaponry with immediate availability of the data to all military personnel on the battlefield.
- ***Context Aware (CoAw):*** *Able to capture knowledge of its surroundings*. The mobile device should be capable of capturing sensory data from its environment. This should include items such as visual data, audio data, motion, precise location, and signals transmitted through the airwaves. Examples from above could include:
    - Location and map data from the military's mobile devices could allow for automatic calculation of gaps in defenses and the level of enemy penetration enabling corrective actions to take place more rapidly.

- Mobile devices could enhance the tracking and identification of legitimate authority figures, criminals, terrorists, and hostile groups within local population from photos in field and facial recognition.

- ***Human Interface (HI):*** *Human interface which provides for the least amount of effort by the user to provide input to the device.* The mobile device should have the capability of providing multiple methods of interacting with the device. The user should be able to choose the method of interacting based on the device, application, and situation. Examples from above could include:
  - The mobile device could allow for automatic verbal translation of local population to increase cooperation.
  - Military personnel could tag key terrain with decisive advantages or key enemy resources to deprive in an augmented reality through gestures.
- ***Data On-Demand (DoDe):*** *Provides for real-time to near-real-time information*. The mobile device should provide a capability to provide information in real-time or near-real-time to the user. Since mobile devices are “always on and on me” devices, the user would also receive the information in near-real-time.
  - Live heads up display with friendly and hostel forces locations.
  - Live status of project progression and road blocks
- ***Individual Assignment (InAs):*** The device has one user that it supports throughout its lifetime. The devices are not shared by multiple users because they are personal mobile devices. They are distributed widely with each user having at least one.

The second category of functionality for mobile devices is “enhanced.” This category of functionality includes utilities performed on our current information systems, but have broadened use cases when implemented on mobile devices.

- ***Information Processing (InPr)*:** The mobile device should provide the capability to process information locally and remotely based on user and application requirements. When remote processing is not available, the applications should provide the capability of local processing when feasible.
- ***Integrated Social Framework (ISF)*:** The mobile device should provide a capability to connect socially, based on user role, to all applications hosted on the device.
- ***Information Fusion (InFu):*** Shares information to authorized devices/users. The mobile device should provide the capability of sharing information with other authorized devices, users, and content providers.
- ***Security Policy Enforcement (SPE):*** Maintains confidentiality, Integrity and availability of the data.
- ***Knows the user (KU) (Has knowledge of the user)*:** The device should have the capability of identifying the user and the role with which the user is currently performing. The device should also have the capability of knowing the user holistically. This would involve the fusion of information as it relates to the user. The device should then be capable of contextually identifying the role under which the user is currently operating. This would also allow the device to execute commands with a higher level of accuracy given the enhanced level detail that mobile devices contains about their user.
- ***Secure Multirole Integration (SMI) (Multiple-personalities)*:** The device is able to support the different roles that a user takes on

throughout the lifetime of the device. The device should be able to maintain the integrity and confidentiality of each roles data, but also be able to display it as desired with as little user intervention as possible.

- ***Dynamic Capability Provisioning (DCP) (Meet the user's perceived needs)*:** The mobile device can provide common functional capabilities. These capabilities would consist of applications the user expects and desires, with the capability of future growth. This growth could come from new functionality or new desires based on the changing needs and roles of the user.

In essence, the mobile devices we describe here create an augmented reality where the user, the situation, user's real environment, and data providers all exist and interact more seamlessly within a network. Thus the "mobile device," although providing much of the functionality of any number of current computing devices, separates itself from these devices in the way it is "personal." The personalization of the device means it brings together a fusion of data as it relates to the individual. It also means there is an expectation of the device always being with the individual and always on or available in a networking sense.

2. Use Case Examples from Functional Objectives

Given the requirements listed above, we envision a number of future-minded use cases that serve to demonstrate the new complexities associated with the information fusion inherent in today's user-oriented, always available mobile devices. Although there are potentially an infinite number of use cases for these devices, we thought the following would provide good illustrations of the multiple-personality use of mobile devices:

- **Integrated Personal Calendar:** As the user rotates through different roles, or personalities, throughout their day the calendar would provide that personality's corresponding schedule or

daybook. These integrated personal calendars could contain scheduling information for private, military, and maybe other roles such as a second job or membership in a professional organization.

- **Geo Tag Photographs:** The user shares photos with geo-location based on the context of the situation. For instance, on vacation the user may want to post photos of their hike through the Appalachian Trail for public consumption. Upon deployment to the battlefield, that same user may want to distribute a geo tagged photograph identifying insurgents on the battlefield using an intelligence application.
- **Geo Location:** On the battlefield the user may want the capability to report Blue Force (i.e. Friendly force) Tracking information, send coordinates to a firebase, or generates intelligence information with geo-location information embedded. When returning home the user may want to provide family members their current location and estimated time of arrival.
- **Video Chat:** The user may want to visually communicate with his family, friends, or colleagues face to face either while deployed or simply away from home, or at home station.
- **Video Teleconference:** The user may need to participate in “face to face” meetings with coworkers who are geographically separate either while deployed or at home station. Much as it is depicted in the “Star Wars” episodes, video teleconferencing could be used to conduct military planning and coordination.
- **Email:** As the user rotates through different roles, or personalities, throughout their day the email inbox would provide that personalities corresponding digital communications. These integrated inboxes could contain digital communication for private, military, and maybe other roles such as a second job or membership in a professional

organization. This would include COI appropriate encryption and digital signing of digital communications.

- **On Demand Contextual Contacts:** The device would maintain contacts and display them within the correct context across all the user's personalities. The user could use the device to remember co-worker names, birthdays, etc. Whereas on the battlefield the device could identify hostile insurgents, or even automatically report sightings of key enemy personnel when spotted.
- **Chat:** As the user rotates through different roles, or personalities, throughout their day the device would provide that personality the correct contacts with which to correspond digitally or chat. These chat sessions could occur with contacts that exist in private, military, and maybe other roles such as a second job or membership in a professional organization.
- **Share space:** The device should provide the user access to shared information stores for each of the user's personalities. For example, the user may want to store information to Google Drive for personal storage and Microsoft SharePoint for work.
- **Real-time Intelligence:** The user receives information, alerts, and advisories, within context, across all personalities. For instance, the user could be alerted when friendly forces nearby engage hostile forces. Based on context, the mobile device could push intelligence information to the user on the locale, such as names of leadership, local laws, and customs when the user is approaching a remote village. At the office, the user could receive weather alerts, new policies, job postings, fire evacuation notices, or just the latest news headlines.
- **Automated Supply:** The user could explicitly or automatically, through the mobile device's context awareness, request resupply or

materiel delivery on the battlefield for delivery. At home, the device could automatically order groceries or home supplies when it detects key items to be “low.”

- **Language Translation:** On vacation or during international meetings automatic translation by the mobile device could be very useful. While on the battlefield, the user could translate orders to or requests from the local populace to include analysis of sign language and facial expressions.
- **Command and Control:** At home station the user could receive the latest direction from leadership through notifications. The user could also contact coworkers, at any time, via a number of communication vehicles such as text, chat, email, social networks, blogs, or voice. In a battlefield situation, the user could send and receive information, such as orders, in the most appropriate vehicle given the context of the situation or ease of use.
- **Remote Health Tracking:** The COI could have the user wear, swallow, or embed a device that transmits personnel data that would not be available otherwise (such as Fitbit [9], M2A capsule, Metria [10]). This could allow remote diagnosis/physicals by doctors, along with constant remote tracking and follow-up. The kind of data that might be obtained is: the number pills taken, number of steps, heart rate, food eaten, body temperature, and sleep quality/quantity.
- **Distributed Sensory Data:** A COI could use a large deployment of mobile devices to collect sensory data to make decisions. Examples of this distributed network would be barometric data for weather forecasting, accelerometer data for earthquake predictions, or accelerometer data for troop or vehicle movements. When

combined with remote health tracking the heath of a corporation, army, or nation could be monitored.

- **Mesh Networking:** The user is able to connect to the network or Internet Service Provider (ISP) by allowing traffic to hop from mobile device to mobile device, with each mobile device essential action as a router. The user could even reach the required information or mobile device without ever reaching an external network or ISP. "Many military systems rely on mesh networking, since forces in the field cannot rely on communications infrastructures. Utilities also use mesh networks for collecting data from equipment, like smart meters." [11]

The above list of uses cases does not detail every possible use for mobile devices by a given user. It does demonstrate that there are unique or enhanced functions enabled by mobile devices. In addition to these unique and enhanced functions, the user may also want to add-on functionality for personal use as new application become available. Therefore, we must provide integration among the multiple personalities based on the user's community of interest. These unique use cases and integration among multiple personalities will be the focus of our analysis and process towards a mobile device security policy for the DoD.

3. Threats and Security Context of Mobile Device Use Cases

Many of the above listed use cases present additional security concerns unique to mobile devices. Unlike laptops, which are typically single purpose use and only used during specific times, mobile devices are personal communication and computing devices that are expected to be always on and always near the user. Further analyzing the use of a laptop versus a mobile device; typically, a user has a laptop issued from their workplace, this laptop is used for work during work times or the occasional home use when the need arises. However, at home they may also have a personal laptop. This personal laptop is used on personal time and only at home or other non-work locations. Note, one can replace

“laptop” with “desktop” but laptops serve the illustration better as they are intended to be more mobile. On the other hand, a mobile device is taken everywhere with the user and used at all times for many different purposes and roles. In essence, the device becomes an extension of the user, a surrogate of sorts for an individual who may maintain several different roles in their life. Using the device for different roles presents significantly complex and unique security concerns.

The complexity of mobile device security for devices which support the above functionality and use cases grows as a result of the differences among COIs and even security requirements among content providers of each COI. Each COI will require an overarching security policy. For instance, a user who is an U.S. Air Force Reservist and a Department of Commerce (DOC) employee would have two COIs, one for each job, on his device. Each COI would have an overarching security policy and each security policy might differ in many ways, especially since the Air Force policy follows the Department of Defense Instruction (DoDI) 8500.2 [12] and the DOC policy follows NIST Special Publication (SP) 800.53 [13] implemented in the DOC information security policies. Additionally, within the COIs there may be content providers which implement more restrictive security policies than the overarching COI security policy. For instance, as a reservist the email content provider may implement a basic security policy whereas a content provider for military medical records would have to implement a more restrictive security policy based on Health Insurance Portability and Accountability Act (HIPPA).

To further demonstrate the need for a security policy that covers the complex security and privacy issues concerning mobile device, an illustration of a few examples and misuse cases have been listed below. The following is a list that exemplifies some of the security policy complexities:

- **User Calendar:** The user calendar is a clear case where the Confidentiality and Integrity of information is important in relation to the COIs. Information from all personalities should be capable of

being displayed in one calendar format for the user but in the case of a military COI the information would not necessarily be sharable with another COI. Additionally, all COIs would not want to allow another COI to alter information. For instance a personal Gmail calendar, although not as concerned about confidentiality, should not allow the military COI to alter the Gmail related calendar information, hence even the Gmail calendar expects a level of integrity.

- **Walk in the Woods:** The walk in the woods example demonstrates that the same functionality for different personalities requires different levels of information assurance. This example starts with a military user on leave walking through a national park. On his walk, he may want to use his Global Positioning System (GPS) for navigation while sharing his progress with photos to his friends and family on a popular social network. That same military user could be deployed a week later to an undisclosed forest. In that forest he would still want to use his GPS for navigation and possibly share photos of tactically or strategically important images. The difference would be that the military photographs should only be shared with his unit and not posted to a popular (or even unpopular) social network. This demonstrates that the same activates generating the same information may require different levels of protection based on context and personality.

- **Crashing a Video Party:** The crashing a video party demonstrates that the functionality offered by mobile devices should be equal across all personalities but separated. This example starts with a military user, on personal time off (PTO), hosting a video conference for a 10 year reunion. It is an open reunion party, so she wants to offer the capability for anyone to drop in and chat. To accommodate this functionality, the service (for example, Google

Chat) displays that she is in a video conference with the option for all contacts to join or drop in. After the reunion, she returns to work and is told to host a video conference for all colleagues on a new work policy. The same functionality must be offered, with the option to join, but she would not want to have the option available for a schoolmate to crash the work video conference.

- **Skyping from a Sensitive Compartmented Information Facility (SCIF):** This example demonstrates that not all functionality should be offered or available at all times. In this example, the user prefers to communicate with friends using Skype and would want it constantly available to him whenever on PTO. When working in a SCIF (in a future environment when mobile devices are allowed in SCIFs), the user would not want to have the capability to purposefully or accidently accept a Skype call from a personal contact.

Along with examples are misuse cases, or example of security issues that could occur on mobile devices. The following is a list of misuse cases that exemplify some of the security policy complexities:

- **Chief Executive Officer (CEO) All Hands for a Harry Potter party:** This example demonstrates that the same command issued to a mobile device will have different meanings based on the context and personality. In this example, a CEO may want to let her entire personal address book know that she is hosting a Harry Potter party, because all of her friends are Harry Potter fans. To accomplish this at home, she tells her phone to email all her contacts that there is a Harry Potter costume party at her house on Friday. If the phone is not aware of the personality and context, then the CEO just invited the entire company over to her house where there will be a lot of colleagues dressed as Hermione and Weasley.

- **Alerting Terrorists of U.S. Friendly Forces:** This example demonstrates the need to protect information presented by the mobile device even when physical control is lost. In this example, a military user has a mobile device that immediately alerts the user of local friendly forces and enemy personnel in the surrounding area. Unfortunately, the user loses their mobile device while on deployment in hostile territory. A local insurgent group finds the mobile device, but cannot unlock it to obtain the device's data. They soon discover that even without unlocking it, they are notified of local friendly forces in the surrounding area. They are also able to obtain a list of individuals who have already been identified as hostile insurgents because of the alerts.
- **Uncontrolled Unclassified Information:** This example demonstrates that defaults for services on the mobile device need to be context and personality aware. When a military civilian receives his new phone, he automatically sets his default cloud storage for personal documents to Microsoft Skydrive. A few moments later, the users receives a work email with an attached Controlled Unclassified Information (CUI) document. The user saves the document to default storage location, which is now Microsoft Skydrive without knowing it. The controlled information is now stored in an uncontrolled commercial service.
- **False Notifications:** This example demonstrates the need to protect against masquerading as another personality or cross another personalities boundary. In this example, the battlefield user downloads a game for personnel use. Unfortunately, the application was develop by unfriendly forces with the intent of providing false notifications to mislead the user in the battlefield. When the user passes by these unfriendly forces, it notifies the user that the unfriendly forces are actually friendly forces and notifies the user

that the friendly forces are unfriendly forces. This causes the user to ignore the unfriendly forces and attacked the friendly forces.

- **Free Wi-Fi on the Battlefield:** This example demonstrates that not all services should be allowed over all possible communication paths. The battlefield user could be offered an astonishing number of diverse services on the battlefield through mobile devices, like Blue Force and hostile insurgents tracking information. If the mobile device defaults to open Wi-Fi access, then all an insurgent would have to do is set up an open Wi-Fi access point and monitor all the data as it traverses the network giving the insurgents critical confidential information.
- **Passwords, there is an App for that:** This example demonstrates the need for enforcement of separation among personalities. The user of the mobile device would like to have a password management tool for their apps on the device, so they go out to the application store and download an app. The tool offers to remember all of their passwords and store them in the cloud for easy recovery. After downloading and installing the app, all the passwords for all personalities are now stored in one application's cloud storage.
- **User Privacy:** This example demonstrates the need for private user data to be inaccessible by the employer. An employee, who is about to leave his second job, sends out his last email of the day on the mobile device provided by his primary employer. After clocking out, he opens up a few chat sessions, on that same mobile device, for his volunteer work with his religious leader and local political leader. Once completing this chat session, he drafts one more email to his therapist complaining about stress prior to retiring for the night. The next day, when he wakes up and returns to his

primary job he finds a termination notice on his desk. This is an extreme example, but there are many not so extreme examples of private data on social networks leading to such a termination.

- **A door to China:** All security starts at the hardware. If there is a backdoor manufactured into the hardware of the device, all the protection mechanisms at the hardware, software, and services levels will be for naught.
- **Silence is information:** This demonstrates the complexities of sensor information among personalities. In this example, two soldiers on the battlefield are about to go on a sensitive mission with their mobile devices. The first soldier, once deployed, has his GPS information provided to a blue force tracking application in his military personality collecting his location and labeling it as sensitive. This first soldier also has the "friend tracking service" application running and collecting the same information while broadcasting it to the Internet. In this example, the second soldier is also running the blue force tracking application, but turns off the "friend tracking service" application once stepping out on her mission. Unfortunately, the "friend tracking service" application still recorded the exact location right before turning off the service. On top of this, the silence of the application alerts the enemies that this second soldier may be performing a sensitive mission.

These examples demonstrate the need for a security policy that covers the complex security and privacy issues concerning mobile devices.

E. SUMMARY

In this section, we have defined the unique aspects of mobile devices. Specifically, we identified mobile device as being more personal. This is made possible since the devices are always on, always on you, and environmentally context aware through their mobile sensors. From these unique aspects of

mobile devices, we identified possible use cases, along with the threats that these use cases present. As we move forward with confronting the security issues of today's mobile devices and beyond, there will be questions about the security of mobile devices that will need to be addressed. These questions include:

1) What is the effect to security policy?
2) Are the security controls affected?
3) How is security implementation affected?

To start this effort, we will further refine and categorize our definition of mobile devices. We will then define a security policy in the perspective of this thesis along with currently applicable policies to mobile devices. From this analysis, we will demonstrate whether organizational policies will need to be modified to accommodate mobile devices. We will use all of this information, and our security policy development methodology, to determine approaches in defining an information flow with the goal of defining security ramifications and possible conflicts.

II. SECURITY POLICY FOR MOBILE DEVICES

A. MOBILE DEVICES

Before moving forward on a security policy, we must define the scope of mobile devices that will be covered in this thesis. In the next few sections we layout three different categories of mobile devices in the order of their evolution towards the ones that we see today (such as smartphones), and beyond. This evolution will start with Handheld Personal Computing Device (HPCD) and then progressively move towards a possible future of mobile devices that include "humanistic intelligence." We will then clarify the scope of this thesis based on this evolution. This scope will be tailored towards HPCDs while trying to accommodate "expandable sensors" and "wearable computing" which are detailed below.

1. Handheld Personal Computing Devices

Handheld Personal Computing Device (HPCD) is the first stage of the mobile evolution covered in this thesis. It is a category of mobile devices characterized by their size or "Hand-Held" status and wireless connectivity. This category of mobile devices usually includes the following minimum characteristics, as defined by NIST and PCMag:

- Single Panel with Touch Screen or buttons
- Portability. Portability creates the need for portable connectivity. It also creates the potential for the device to be present in environments not supportive of the data processed, stored, and transmitted.
- An operating system optimized for mobility with a single user. OS Security primarily provides protection for the commercial service provider.

- At least one wireless/wired network interface for Internet access (data communications). This interface could use Wi-Fi, cellular networking, Bluetooth, WiMax, Near Field Communications (NFC), USB, or other technologies that connect the mobile device to network infrastructures with Internet connectivity.
- Local built-in (non-removable) data storage
- Built-in features for synchronizing local data with a remote location (desktop or laptop computer, organization servers, telecommunications provider servers, other third party servers, etc.)
- From this minimum set of characteristics, HPCDs can be further reduced into two categories: fixed function or general purpose.

Fixed function or single purpose HPCDs were the first generation of mobile devices to market, and still flourish today. These devices perform one specific application well. As such, these devices only have the wireless protocols, applications, and sensors needed to perform that single application or function. Examples of these devices would be the Amazon Kindle Paperwhite (eReaders), Garmin handheld Global Positioning Systems (GPSs), handheld video phones, and portable media players. These devices cannot perform all the functions of a general purpose HPCDs, but they can usually perform their one specific application reliably.

The second category, general purpose HPCDs, are designed to be a platform for multiple applications. They are designed to be expandable beyond the default applications that reside on the device at the time of purchase. Examples include iPod, iPhone, iPad, Android Devices, and Microsoft Surface. As such, they usually have the following additional minimum characteristics:

- At least one wireless interface (such as Wi-Fi, Bluetooth, NFC), sensors (camera, microphone, GPS, barometer, accelerometer) that provide data about its surroundings, and actuators (e.g., speaker) that would not be available otherwise.

- Applications available through multiple methods that expand the device beyond its originally provided applications

It was the creation of these general purpose HPCDs that revolutionized the commercial marketplace. It allowed for the ability to create and easily distribute a single purpose application (such as GPS or e-reader) on a general purpose HPCD (such as smartphone or tablet) through an application marketplace onto a device already owned by the user. This is accomplished at a fraction of the cost of a single purpose HPCD by using functionality and embedded sensors already provided by the device. These applications harvest data from available embedded sensors on the mobile device, such as GPS for mapping jogging routes. These applications eventually evolved to interface with external devices, beyond the ones built into the mobile device (e.g., sensors). These additional sensors are used to collect more information about the device's soundings. This in turn broadens functionality beyond what the mobile device could initially provide at purchase. An application marketplace and integrated sensors distinguish a general purpose HPCD.

It is important to have a basic understanding of these topics:

a. Application Marketplace

The application marketplace provides access to addition software applications to expand the functionality of the device. It is usually a service provided by the Operating System (OS) developer or device manufacture that has the capability of presenting applications available for the user to install. In doing so, "The application market place function combines the traditional roles of content aggregator and distributor. The store constitutes a direct link between developers and consumers, significantly reducing the barriers between them, as both interact directly with it" [14].

b. Embedded and Expandable Sensors

As stated earlier, mobile device applications are increasing their functionality by using sensors connected to the device. This connection is accomplished through sensors that are either embedded (such as GPS, camera, accelerometer), wireless (such as Wi-Fi, Bluetooth, NFC) or via some external interface, for example a dock. Examples of such applications using these sensors include Square's mobile payment [15] (docked connection) and QR codes (data sensed through embedded camera). There are many drivers for this expansion of the kinds of sensors and their use, but "one of the biggest drivers … is the increasing number of low-cost sensors available for many different kinds of functionality" [16]. "Some of the standard sensors include movement (via accelerometer), sound, light, [user input or relative position] (via potentiometer), temperature, moisture, location (via GPS), heart rate and heart rate variability, and GSR (galvanic skin response or skin conductivity)" [16]. "Many devices have been attached to smartphones for novel applications.. such as AliveCor's electrocardiogram (ECG) recorder for heart monitoring, MobiSante's smartphone-based ultrasound imaging system, and the CellScope. The CellScope has a series of clip-on modules for the smartphone such as an otoscope (to look into the middle ear), and a dermascope (to capture magnified images of the skin)" [16]. All of these applications using these embedded and expandable sensors are leading to the next generation of mobile computing.

> The next generation [of mobile computing]… is visible in product announcements, many of which fall into the category of wearable electronics and/or multi-sensor platforms. These products include smartwatches, wristband sensors, wearable sensor patches, artificial reality-augmented glasses, brain computer interfaces, wearable body metric textiles (such as Hexoskin to track athletes performance). [16]

2. Wearable Computing

Wearable computing is a next logical step and extension from HPCDs. "An important distinction between wearable computers and ...handheld computers…

is that the goal of wearable computing is to position or contextualize the computer in such a way that the human and computer are inextricably intertwined" [17]. Currently there are three wearable computing categories available or publicized as being under development. These categories are augmented reality, wearable human sensors, and smart clothing.

As documented in Microsoft's patent filling, the augmented reality display "is a system and method to present a user... with supplemental information when viewing a live event. A user... views the live event while simultaneously receiving information on objects, including people, within the user's field of view... The information is presented in a position in the.. display which does not interfere with the user's enjoyment of the live event" [18]. They are devices that "let you show and interact with the world around you without disconnecting from it" [19]. Another example of the functionality provided by such augmented reality devices was documented in Time magazine. The commented about Google Glass that, "Users will be able to take and share photos, video-chat, check appointments and access maps and the Web" [20]. A potential example of map notifications is demonstrated in Figure 1.

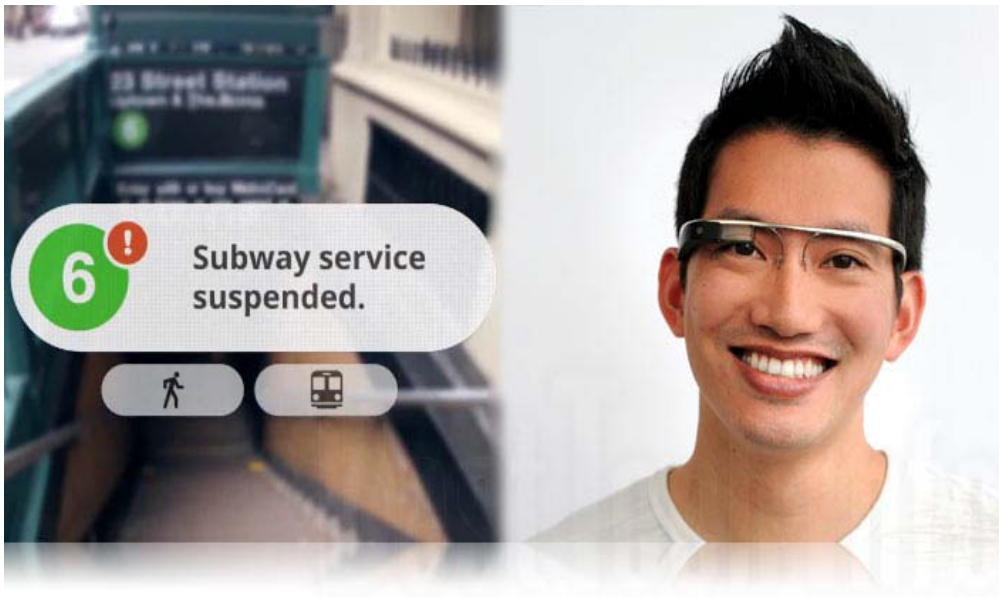

Figure 1. Example Notification from Google Glass. From [21]

“The see-through lens could display everything from text messages to maps to reminders. They may be capable of showing video chats, providing turn-by-turn directions, taking photos and recording notes—all through simple voice commands” [22]. A potential example of Turn-by-Turn direction functionality is demonstrated in Figure 2.

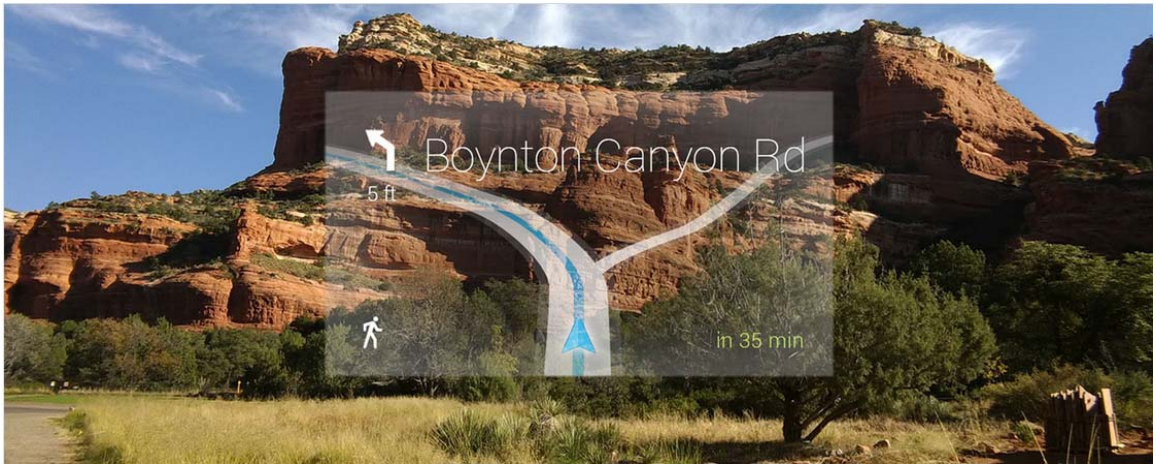

Figure 2. Example Turn-by-Turn directions. From [23]

These glasses could eventually evolve into a contact lens that is placed into the eye directly, therefore alleviating the need for headwear. In fact, “The Centre of Microsystems Technology (CMST) has developed an innovative spherical curved [Liquid Crystal Display (LCD)] display, which can be embedded in contact lenses. In the future, the display could also function as a head-up display, superimposing an image onto the user’s normal view” [24] .

“Another new product category that could quickly become commonplace is wearable sensors, low-cost disposable patches that are worn continuously for days at a time and then discarded. It is estimated that 80 million wearable sensors will be in use for health-related applications by 2017, an eight-fold increase over today” [13]. “The concept is not new, nicotine patches for smoking cessation are a familiar concept, but the extended on-board sensor functionality is an important innovation. The next generation of patches moves away from standard transdermal passive diffusion technology, and instead uses rich sensor

technology to enable patches to transmit information wirelessly, and possibly engage in two-way communication for real-time adjustments. One of the potential developments in wearable patches is Sano Intelligence's continuous blood chemistry monitoring patches. The disposable patch (one-week use) has been demonstrated to measure blood glucose and potassium levels, and aims to measure a full metabolic panel, including kidney function and electrolyte balance. Further, there are enough probes on the wireless, battery-powered chip to continuously test up to a hundred different samples" [14]. Other examples of wearable sensors include Scandu SCOUT [25] (medical biometric), Fitbit [9] (wireless health tracker), M2A capsule (wireless endoscopy pill), and Metria [10] (remote medical monitoring system). Notice that many of these uses are based on health monitoring and have privacy information consequences, this will be important as we move forward with the security policy for mobile devices.

The final wearable computing item to be discussed in this document is "smart clothing." Examples of such items include the Army's Antenna Clothing which "could reduce the burden and the danger for military radiomen" [26] and nike+ running shoes for tracking fitness. There is also **"**a new product category, the smartwatch, which is effectively a wearable connected computer. This new generation of programmable watches includes the Pebble watch, the Basis watch, the Contour Watch from Wimm Labs, and the Sony SmartWatch" [16]. As these wearable computers are integrated into our everyday life, slowly the human and machine begin to intertwine leading to humanistic intelligence.

3. Humanistic Intelligence–Embedded Technology

"One of the main features of humanistic intelligence is constancy of interaction, that the human and computer are inextricably intertwined. This arises from constancy of interaction between the human and computer, i.e., there is no need to turn the device on prior to engaging it (thus, serendipity)" [17]. "Another feature of humanistic intelligence is the ability to multi-task. It is not necessary for a person to stop what they are doing to use a wearable computer because it is

always running in the background, so as to augment or mediate the human's interactions. Wearable computers can be incorporated by the user to act like a prosthetic, thus forming a true extension of the user's mind and body" [17].

All three different categories of mobile devices listed above have their own particular security requirements and concerns. In order to move forward, we will focus our scope on the kind of mobile device we will be discussing for the remainder of this document. Our scope will be tailored towards HPCDs while trying to accommodate "expandable sensors" and "wearable computing." With the scope of mobile devices decided, we will need to define and scope a security policy.

B. WHAT IS A "SECURITY POLICY"

1. Defining "Security Policy"

In his book, *Computer Security Art and Science*, Matt Bishop describes a security policy as, "a statement of what is, and what is not, allowed" [27]. In the field of Computer Science, the term "security policy" is well used. The issue with "security policy" is it has many different meanings depending on the context. The online Webster's dictionary defines "Security" as the quality or state of being secure. Their second definition of the word "Secure" is free from danger, free from risk of loss, affording safety, and/or trustworthy and dependable. Therefore, one can deduce a security policy to be: A policy which, if followed, would keep the object of the policy in a quality or state of being secure, which is to say it would be kept free from danger, loss, kept safe, and is considered trustworthy and dependable. In the case of an information security policy, we assert the object is information. Finally, one could compare the concept of being "free from danger and loss" to the idea of maintaining confidentiality. "Safety and trustworthiness" could describe Integrity. Finally, "dependable" could describe Availability.

In the DoD there are many contexts for security policies. Two such contexts would be physical security and information security policies. What is

interesting is the two overlap in requirements. For instance, physical security and information security although seemingly very distinct, are, in fact, symbiotic in their relationship. One can imagine that without good physical security, information would be easy to obtain by simply taking the physical devices on which the information is stored. In reverse, good physical security would be severely compromised if the enemy had access to our information. Imagine what would happen if the security guard's relief schedules, building drawings, or distress code words were known to the enemy. In this case, the insecurity of information would compromise our physical security. Although a coordinated and comprehensive security policy is required at the DoD level, this paper will focus on security policy from the context of information security. Although, as noted, information security must identify physical security requirements as they relate to the protection of information.

2. Information as the Transactional Entity

If we apply Bishop's definition to information security we have a good abstract concept for a DoD information security policy, however, we still fail to link this concept to the overall purpose. For illustration, we suggest there exist four primary categories for Information Security implementers: government organizations, commercial organizations, private organizations, and individuals. The specific purpose and intent of a given information security policy comes from the specific needs of an organization or individual. Table 1 outlines a partial list of motivations for employing a security policy for each category of beneficiaries:

Category of Information Security Policy Beneficiaries	Resource
Government Organizations	*National Security Information, Critical Information Indicators (OPSEC), Physical Security Information (Protection of property and Equipment), Personally Identifiable Information (PII), Proprietary Information, Financial Information
Commercial Organization	*Financial Information (Profit and Proprietary Information), Proprietary Information, Physical Security Information (Protection of property Equipment and employees), Employee PII
Non-Commercial Organizations (Charities, Professional Organizations, Non-profit Special Interest Groups, etc.)	*Financial Information (but here in the context of meeting the Organization's Objectives), Proprietary Information, Physical Security Information (Protection of property Equipment and employees), Employee/Member PII
Individuals	*PII, Personal/Family Security Information, Financial Information

* denotes the primary resource

Table 1. Purpose of a Security Policy

The main purpose of an information security policy depends on the data owner (or stakeholders) but it revolves around information, just different categories of information. A Government organization, such as the DoD, is primarily concerned with national security, and thereby must protect national security information. More specifically our nation has become aware of the requirement for cybersecurity [28], where information is considered a vital resource that requires protection and availability. Commercial organizations have requirements to meet certain laws, but most importantly, their requirements derive from the need to profit. Therefore, commercial organizations are concerned mostly with the integrity of their financial information or information related to the financial health of the company. Individuals on the other hand are

primarily concerned with privacy in order to protect themselves, their family, their belongings, and their financial well-being. Confidentiality of personally identifiable information (PII) is key to an individual's ability to that protection. Non-commercial organizations have many of the same concerns as commercial organizations and individuals combined. They do not have profit but they do typically have an operating budget that is essential to meeting the goals of the organization. Stated another way, both individuals and groups of individuals (organizations) have implied or stated missions. For individuals, their mission is life and the pursuit of happiness. Organizations have specific missions that further their member's individual missions. In some cases, the missions involve acquiring money that can be exchanged for supporting life and pursuing happiness. Both individuals and organizations need sufficient privacy/secrecy for mission accomplishment. The common element is information.

We assert the central purpose of an information security policy is to define where information is allowed and not allowed to flow, where information must be allowed to flow, and who or what can and cannot create or edit information. It would help to think of information as what we will call the transactional entity. As noted in the previous paragraph, information is the central element in all cases. Therefore, information is in fact what we wish to guarantee and control in order to meet the purpose and intent of the organization and individual. We can guarantee the flow of information and control the flow of information by developing an information-flow centric information security policy. A policy describes where information flow is allowed and disallowed and where information must be guaranteed to flow. In this manner, we will say information-flow is the vehicle through which we will meet our organization or individual objectives.

3. Security Objectives and Resources

We believe the need for an information flow is derived from objectives an individual or an organization is trying to achieve. Controlling and assuring the

flow of information or enforcing an information-flow policy without clear objectives could be wasteful. In the case of a commercial organization, for instance, being too wasteful in security could produce the opposite result of the purpose to produce profit by needlessly increasing cost. For government organizations, there is also a concern for cost, but there may also be a negative effect on the mission when information essential to the success of a mission may not be readily available to the mission planners or executers because of an overly restrictive information-flow. On the other hand, information flow enforcement must meet all the intended purposes in order to protect the person or organization. Therefore, the information-flow should be tied to the purpose via the use of policy objectives. These objectives must clearly identify how they (the policies) meet the intent of the organizational or individual purpose. This construct, built with objectives, will link our information flow to our purpose to create a comprehensive information security policy that matches the overall intent and nothing more.

Daniel Sterne, who noted the multiplicity in the common meaning of the term “Security Policy” sought to define new terms with which we could more precisely discuss security. In his paper, *On the buzzword “Security Policy,”* he attempted to bridge the gap of all security policies by defining the term “Security Policy Objective.” In the security policy objective, the data owner defines the intent to protect an identified resource from unauthorized use. He also states the resource must have some form that is tangible. Overall, the security policy object is a description of the kinds of uses that are to be regulated. This is Sterne’s description of the abstract policy, which describes a statement of intent [29]. However, it is too narrow in that it does not address guaranteed levels of service. We will also more clearly define “tangible” resources and the objectives for our definition of a security policy.

Resources can be divided abstractly into five main categories: people, equipment, material, financial implements, and information. These resources could be physical, such as raw material, or abstract such as money or company

stocks. It is important to consider information as an independent resource. For instance, in the world of Psychological Operations (Psyop) where, from a security perspective, it is very important to maintain positive influence on one's own troops, a person's feelings would not be tangible or stored in an IT device and yet a PSYOP operator must implement ways to protect friendly forces from being swayed by enemy Psychological attacks. In another example, intelligence information is not always manifested in an IT device. As a first hand witness, one could pass on sensitive information verbally to another person. This passing of information should be disallowed by policy. So one may protect other resources by controlling the flow of information but information is also the object of protection as a resource in itself.

Objectives also have three main categories that are well defined as the CIA information security triad: Confidentiality, Integrity, and Availability. We assert, that in relation to a particular resource, an information security policy statement should include an objective which defines how we are keeping information confidential, maintaining its integrity, and/or guaranteeing a level of service (availability).

4. Defining "Information Security Policy"

In our understanding of a security policy consider a combination of both Bishop's and Sterne's explanation. We will modify Sterne's security policy objective to mean a single statement of a particular allowed or disallowed interaction between subjects and objects. Both subjects and objects can be tangible or intangible. Subjects can also be objects and vice versa. This way we incorporate the simplicity of Bishop's definition of what is allowed and disallowed and we add more specificity as to what we are protecting as is suggested in Sterne's paper.

However, this definition fails to link the "what" to the "why." The "why" is the intent, or as Sterne might say, the objective. Additionally, the term "interaction" as it relates to information is too ambiguous. Within the intended

policy, information can be used many times but not be revealed. For example, information about DoD intelligence can often be known and acted on, but the intelligence itself may not be provided to other individuals. Further complicating the issue, information when acted on may also compromise the intelligence that spurred it and thereby reveal the information. In this case, the security policy may need to describe uses of knowledge gained from intelligence information. What is common in both these examples is the flow of information.

A more accurate definition of an information security policy was provided by Dr. Dinolt, “[An Information security policy] is a verbal description of allowed and/or disallowed information flow, it may be mandatory or discretionary access control, it may be for information privacy and/or integrity, and may provide provision of service guarantees” [30]. Adding the “how,” we define an information security policy statement as, “A verbal description of mandatory or discretionary access control to define allowed, disallowed information flow, and/or service guarantees for the purpose of protecting an identified resource.

There are three main components of an information security policy statement. These characteristics are instantiated in the policy. The first component is the access control in terms of Mandatory Access Control (MAC) and Discretionary Access Control (DAC). The second component is the objective(s) in terms of Confidentiality, Integrity, and Availability as discussed previously. The third component is the resource(s) intended to be protected by the policy statement. An information security policy statement would not be complete if it did not describe all three components. An information security policy is a collection of security policy statements. A collection of all information security polices for a given organization are what we will call Organization Security Policy (OSP). It might be useful to follow some sort of thought process in order to fill out all the required objectives. A typical process is:

1) Identify and categorize your resources.

2) Identify which resources require protection and how in terms of CIA objectives.

3) What behavior must be imposed in order to meet the CIA objectives to be satisfied?

Figure 3 shows an abstract construction of an information security policy statement, security policies and organizational security policies.

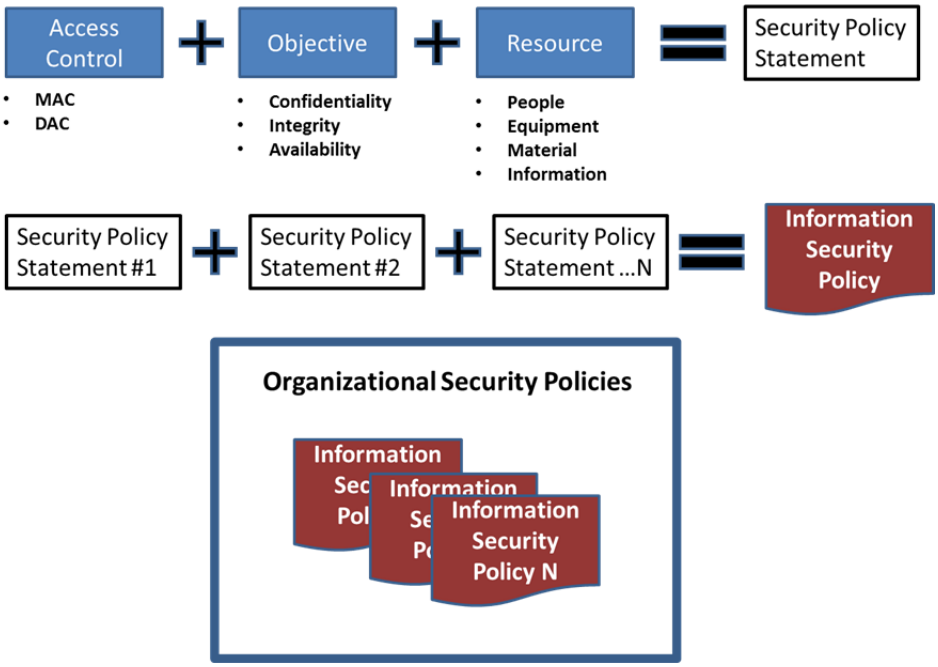

Figure 3. Information Security Policy Statement

A complete security policy statement requires all components be clearly defined in prose and can be written in any order. In an example, an information security policy statement may be, “National Security information shall be protected from unauthorized disclosure and modification by restricting access to only those with the appropriate security clearance, a signed non-disclosure agreement, and demonstrated need-to know.” This statement, modified from the Department of Defense Directive (DoDD) 8500.01E [31], contains all the required components of an information security policy statement. The access control is MAC with DAC tacked on top as personnel are given access only after they meet

certain published criteria such as obtaining the appropriate clearance but are further restricted by a “demonstrated need-to know” which is determined by the person who is providing access to the information, but is not specific to the type or label of the information. The resource is “National Security Information,” and the objective is to maintain the confidentiality and Integrity of National Security Information. Of course, “National Security Information” and “appropriate security clearance” must and would be defined. The most important aspect is ensuring the information security policy includes the three basic elements, in any order, without providing the “how,” more than is needed to understand the access control. To this point, too much information is unwanted at this level. For instance, if the statement had included a requirement for encryption, as is found in the DoDD 8500 series, this would be too specific, it would be the “how.” A requirement such as encryption is a specific implementation, which is better defined at a level of implementation closer to the specific device. Therefore, information security policies are “supported” by implementations. In the DoD these lower levels are in general the Security Technical Implementation Guide (STIGs) and their corresponding automated benchmarks [32]. The other federal construct is the NIST SP 800.53 controls and the Security Baseline Configuration Guides, some of which are defined with government-wide configuration guides such as the United States Government Configuration Baseline (USGCB), formally Federal Desktop Core Configuration (FDCC).

C. SECURITY POLICY DEVELOPMENT METHODOLOGY

1. Security Policy Levels and Examples

In the previous section, we draw on Daniel Sterne’s terminology for the “Organization Security Policy (OSP)” and “Security Policy Objective.” Except Sterne describes an OSP broadly, where the concept bridges policy with elements of implementation. Specifically in Sterne’s paper, there is no clear concept of security controls. We choose to add in security controls in order to

describe, in more detail, how one must implement the OSP. In doing so we use the NIST SP 800.53 terminology. Figure 4 describes our concept.

Figure 4. Information Security Requirements Hiearchy

The security policy objectives give us our intent, which is defined within the OSP as described in the previous section. The security controls provide how the OSP is satisfied, which must then be specifically translated into the technical requirements and operation procedures for both specific information systems and situations (Table 2).

We differ from NIST in that we believe management controls overlap and are consumed by the OSP. In the NIST Risk Management Framework (RMF), security controls seem take on an all-encompassing role in not only driving downward to device specific implementation but driving upward to policy requirements as well. Security controls are organized as follows.

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

Table 2. NIST Security Controls. From [13]

First, one might think the management controls contain all the policy requirements. In fact, management controls provide for the management functions of the risk management framework for the organization. Second, every control family starts with a requirement to have policies and procedures addressing that family of controls. We believe this organization causes a bit of confusion. In practice, there becomes an overly complicated and circular relationship between controls and organizational policy that then includes higher level policies. It is unclear whether an organization must produce policy at their level or if they can assume the policy of a higher organization. The usual result within federal agencies is a whole policy set at each major organizational level that simply regurgitates the NIST SP 800.53 revision 3 controls.

Therefore, we choose to remove management as a class of security controls. Which is what appears to be taking place in the revision 4 of the SP

800–53 [33] document currently in draft as the document makes no reference to the class of the control. In the modification we propose, we assume the NIST management class would be assumed within both the operational and technical controls, not just simply disregarded. Additionally, we believe each security control should be clear in its intent. There should be an automated or procedural implementation. Operational controls should be procedural whereas the technical controls should be implemented automatically by the given information system or collection of systems. That is not to say an operational control could not compensate for the lack of a device's ability to implement a technical control. However, it should be noted that the technical control was not implemented rather than considered satisfied by the procedure. This distinction will help in determining the exact nature of an information system's ability to implement the OSP. Finally, it is assumed that it is in place to support a security control and therefor this circular reference should be removed from the controls. In our approach, we assume that if there is no policy-objective statement that requires the use of a particular control then it is in fact not required.

Sterne does very well to define technical controls. Automated Security Policies (ASP) as he described are automated implementation of the OSP. However, he fails to clearly address any concept for what we would call operational controls. Believing the procedural element of information security is as important, if not more, than the automated controls, we choose to define our security control layer in two classes: operational and technical. At the device specific implementation level we translate operational controls to procedures that are implemented by humans, and technical controls which are implemented as benchmarks on computers. We borrow the term benchmark from the Defense Information Systems Agency's (DISA's) automated portion of technical specifications (e.g., STIGs) in compliance with NIST Security Content Automation Protocol (SCAP) specifications [32]. SCAP is a suite of specifications that standardize the format and nomenclature by which security software products communicate software flaw and security configuration information [34].

Considering our modification of Sterne's definitions and NIST's security control construct, we have now defined the following information security construct (Figure 5).

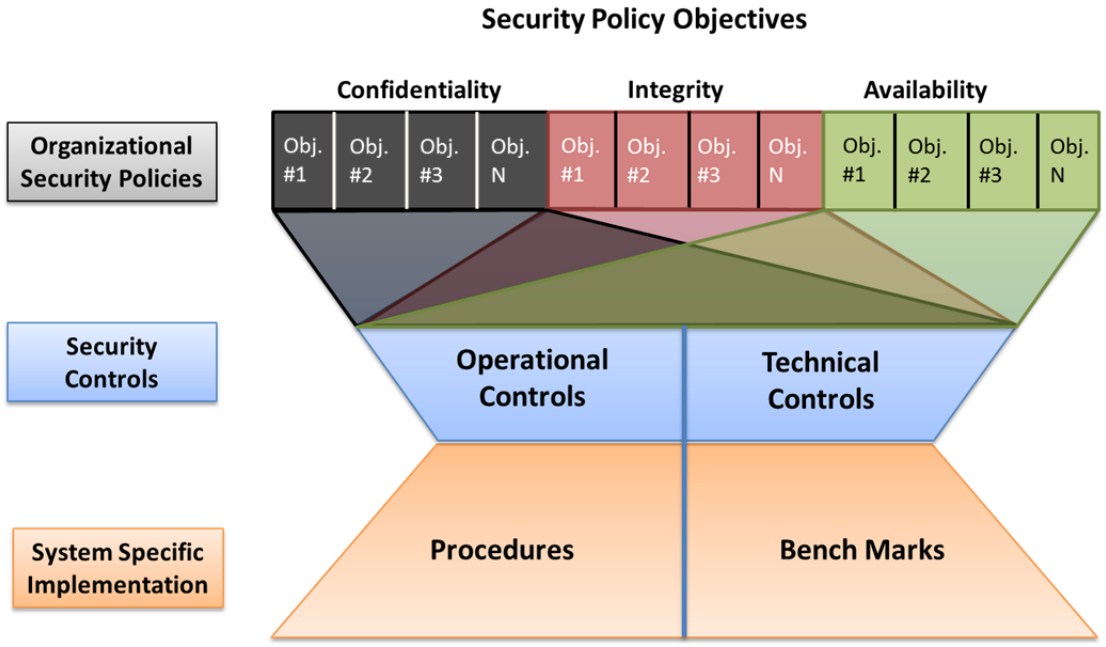

Figure 5. Information Security Construct

Our information security framework is divided into three main levels:

- **Organizational Security Policies (OSP)**, which collectively describe the information-flow policy
- **Security Controls**, which provide the how
- **System Specific Implementation**, which fills in the details for a given information system or logically grouped collection of systems

In our framework we create organizational security policies with information security policy objective statements. Security control baselines are developed based on the security policy objectives and mapped to the objective statements in order to ensure complete coverage. In turn, at the information system level the device benchmarks map to the technical controls and procedures map to the operation controls. In this way, one can ensure there is

complete coverage of all controls by the system specific implementation and there is complete coverage of the OSP by security controls. In other words, every system specific implementation can be mapped to the specific security policy objective statements it supports and each security policy objective statement can be linked to the resulting device specific implementations. This allows one to show complete coverage of the OSPs and complete requirements traceability.

Starting with our previous security policy objective example, a mapping would look like the Figure 6. Of course, this example does not include all branches of the possible many to many relationships, it is simply an example for illustration.

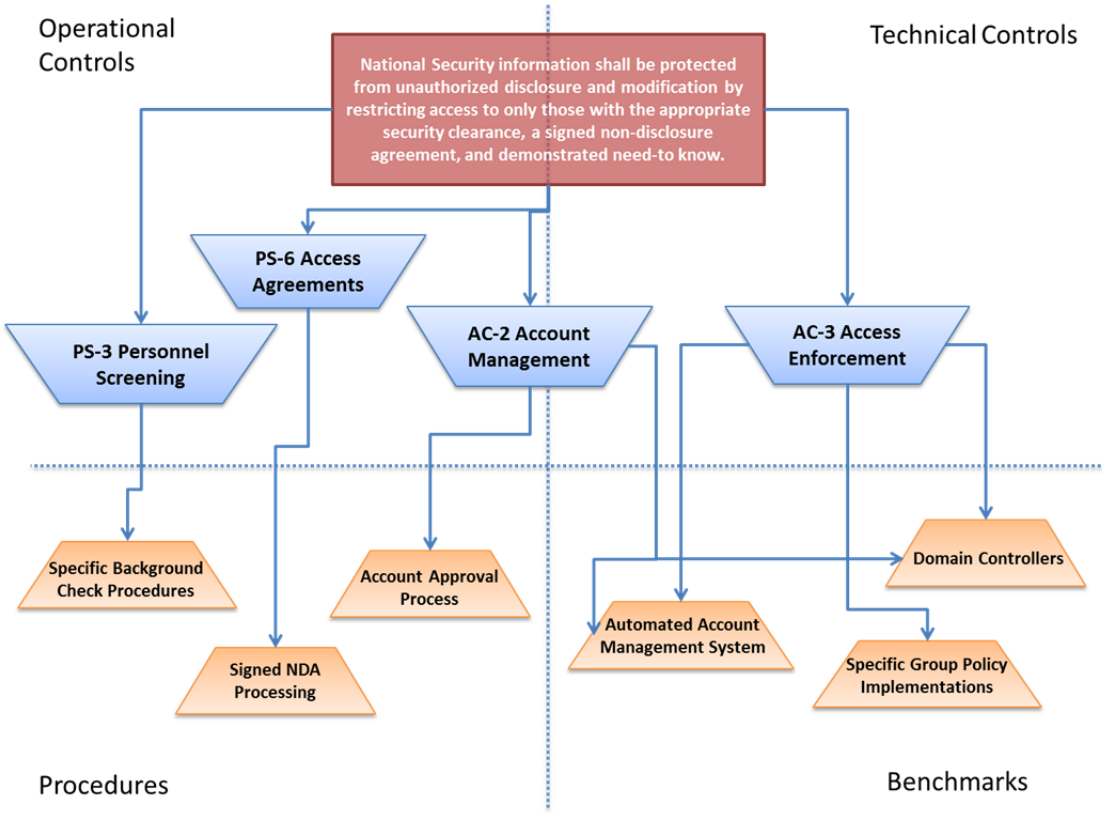

Figure 6. Example Information Security Construct Requirements Traceability

In Figure 6, we show how a security policy objective should be mapped to specific implementations. In this example the implementation are generalized, but in practice they would be very specific. For instance, instead of the benchmark being “Specific Group Policy Implementations” the benchmark would be all the specific settings for the given device as identified in the Baseline Security Configuration Guide. In DoD, these guides are the STIGs and the SCAP benchmarks. An example of a specific setting would be: set “Accounts: Guest Account Status” to “Disabled.” There is a large number of these settings that are required, many of which may map to multiple controls. Also, in our example we show the control AC-2 as bridging the operational and technical controls. This is because at the sub-control level this control had elements of both. There is an initial and continuous process for approving accounts and there are sub-controls that require automated management such as automated disabling of accounts that remain dormant for a given period of time. In the case of a windows domain,

the automated disabling of a dormant account is a specific setting on the domain controller. Therefore, this sub-control translates to benchmarks. Although the example is generalized at the control level to save space, in practice a sub-control should be clearly intended for either procedural or benchmark implementation. There may also be cases where a system cannot implement certain technical controls either wholly or partially. In those cases it must be determined if an operational control and/or procedure can compensate for the lack of functionality. Otherwise, the system will not be able to meet the driving information security objective.

Ultimately, the goal is to meet all the information security policy objectives. To do so we must be able to determine what requirements an information system must meet. Therefore, we must be able derive specific security implementations from the information security policy objectives. Our construct is an attempt to clarify this relationship and provide a 3-level framework for determining systems specific requirements. However, in the details of developing system specific requirements, we believe one must follow an engineering process.

2. Engineering Process

In order to develop a security policy, engineering processes must be selected. The NIST Risk Management Framework (RMF), diagramed below, is the one we chose since a majority of this thesis is based on their document. The RMF consists of six steps to be followed throughout an information system's life cycle. Since we are focusing on the creation and implementation of a security policy for mobile devices, we will focus the Categorize step through the Implement step (Figure 7).

Engineering Process

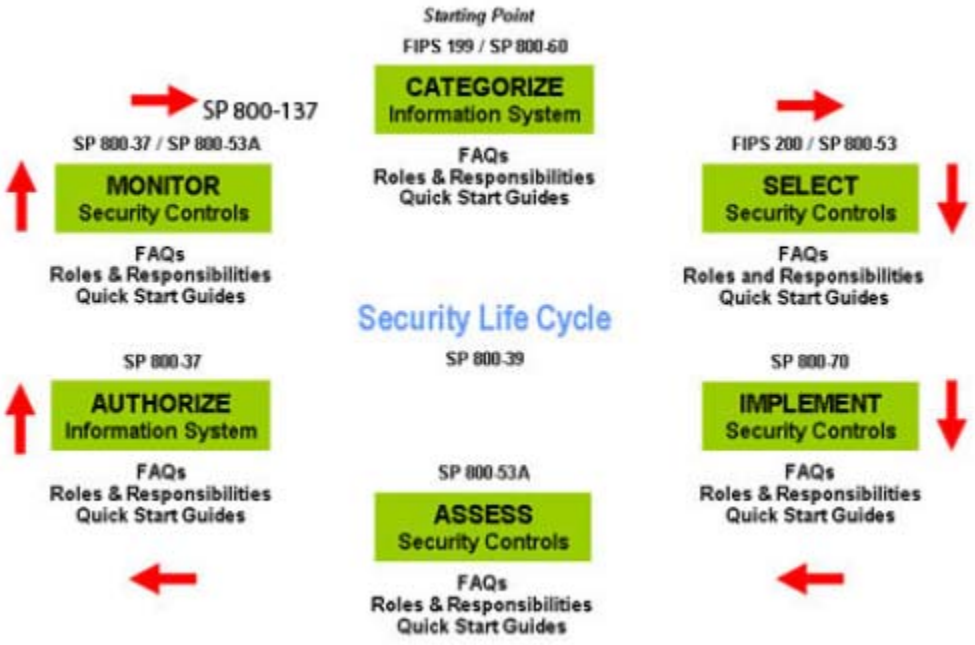

Figure 7. Engineering Process in the NIST RMF

Prior to the Categorize step of the RMF being executed, preparation must take place and requirement analysis performed. This preparation begins with the collection and consideration of architecture descriptions and organizational inputs. The organizational inputs that should be consider include [35] :

- Laws, Directives, and Policy Guidance
- Strategic Goals
- Objectives and Priorities
- Resource Availability
- Supply Chain Considerations

The architecture descriptions that should be considered include [35]:

- Architecture Reference Models
- Segment/Solution Architectures

- Mission/Business Processes
- Information System Boundaries

These inputs are utilized to perform requirements analysis. Requirements analysis would include identifying the needs of the organization (what the product must do) and the security requirements for the product (e.g., relevant security policies) [36]. The end user's requirements, such as remote access for telecommuters or a web server to make internal information available to employees are identified upfront in the requirements analysis. The results of preparation should be documented in for inclusion of Categorize step of the RMF.

The Categorize step of the RMF is performed after the architecture descriptions, organizational inputs, and requirements are defined. This step starts with identifying all the information types for the system. This involves identifying all of the applicable information types that are representative of data input, stored, processed, and/or output from each system [37]. These information types are then used to establish provisional impact levels based on Federal Information Processing Standard (FIPS) 199 [38] categorization criteria. The provisional impact levels are then reviewed and adjusted based on the security objectives of each information type. After the review is completed, the process described in FIPS 199 is used to determine the system security categorization level (low, moderate, or high) which is used for selecting the security control baseline in the Select step [37].

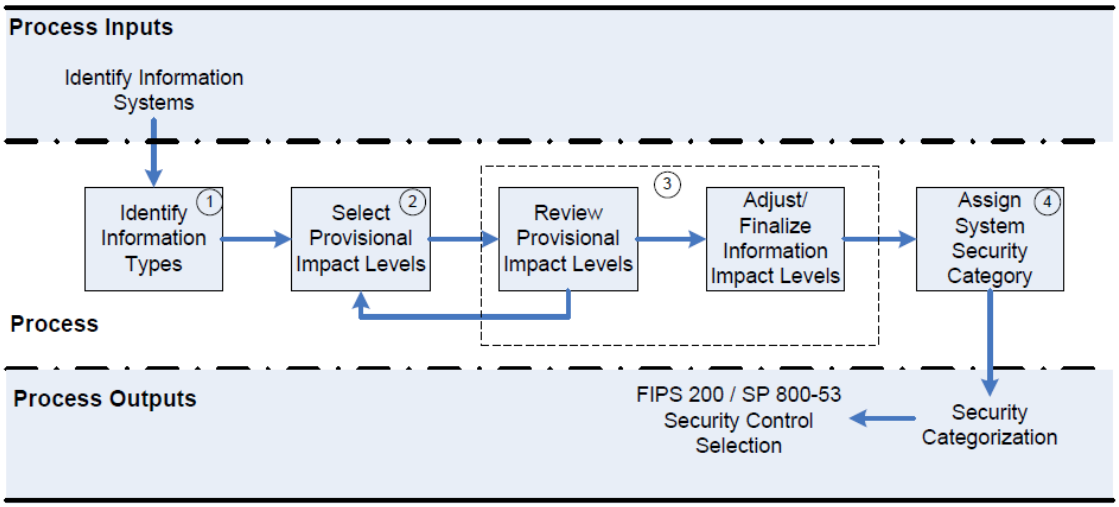

Figure 8. SP 800–60 Security Categorization Process Execution. From [37]

In the next step of the RMF, Select, we select an initial set of baseline security controls for the information system in accordance with FIPS 200 [39] and NIST SP 800–53. The derived impact level (low, moderate, or high) obtained from the Categorize step, is used to select the appropriately tailored set of baseline security controls in NIST SP 800–53 [13]. After selecting the initial set of baseline security controls, they are then tailored to more closely align with the specific conditions within the organization [40]. Finally, a risk assessment is performed against the tailored security controls to determine if additional supplementary controls are required to mitigate unacceptable risk. During this stage, threats to the information system are identified. A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. The goal of this stage is to identify potential threat-sources that are applicable to the information system being considered, as well as the vulnerabilities that could be exploited by the potential threat-sources [36]. In many cases, additional security controls or control enhancements will be needed to address specific threats to and vulnerabilities in informant systems [13].

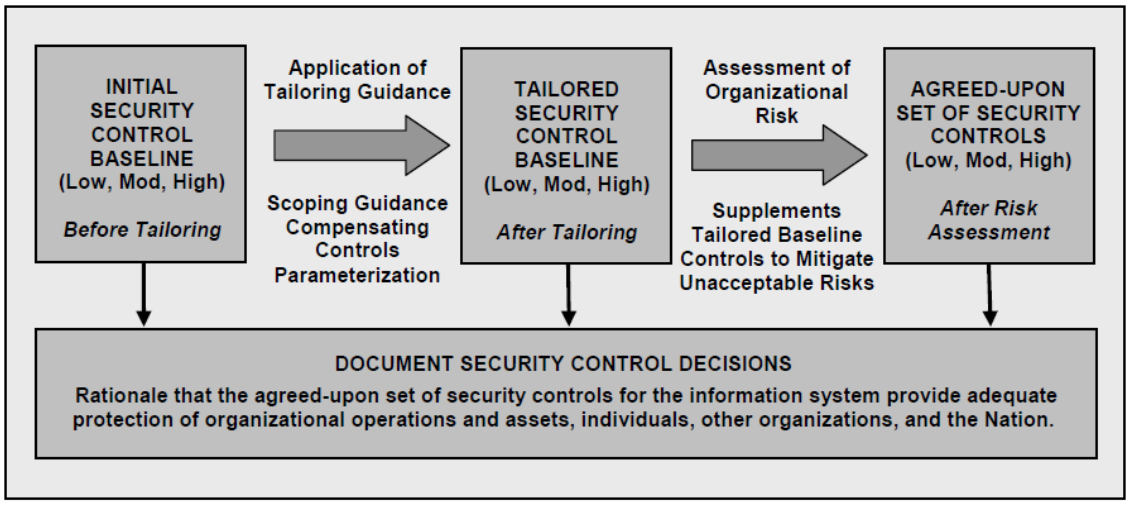

Figure 9. Security Control Selection Process. From [13]

In the Implement step of the RMF, we implement the security controls and document how the controls are deployed within the information system and environment of operation [40]. It is important to note that this step of the process is currently being updated by NIST in SP 800–160, but for now we will use SP 800–70 for this stage. During this stage, security controls targeted for deployment within the information system are allocated to specific system components responsible for providing a particular security capability [35]. In this step it is necessary to ensure that the security controls selected are appropriate; that is, that they implement an appropriate security solution and still allow the system to meet its requirements for functionality [36]. Once deemed appropriate, security controls are deployed or implemented within the information system and appropriately documented. In addition to deploying the selected security controls, organizations ensure that mandatory configuration settings are established and implemented on information technology products in accordance with federal and organizational policies (see diagram below) [35].

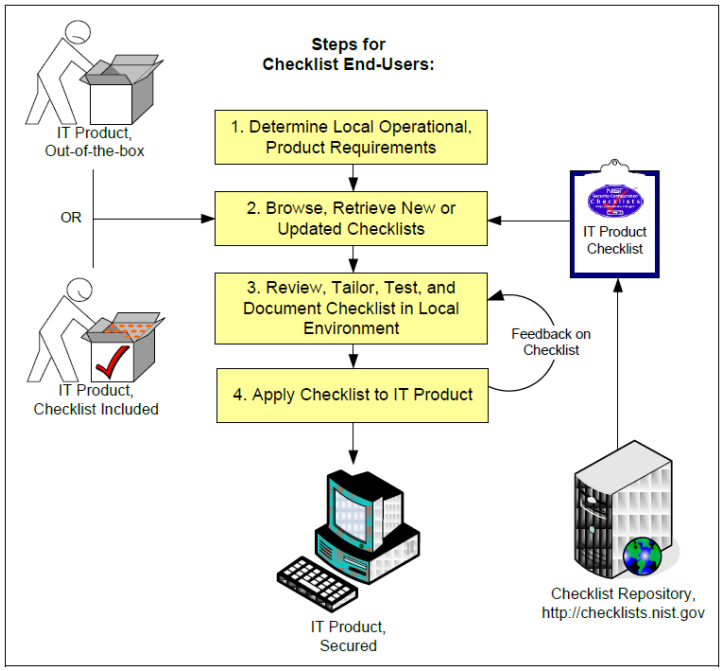

Figure 10. Checklist User Process Overview. From [36]

During this processes the mandatory configuration settings, or checklists, are also used to analyze the impact on an organization's current policies and practices (e.g., having JavaScript disabled in a browser might make some web pages unusable). An organization may determine that some aspects of the checklist do not conform to certain organization-specific security and operational needs and requirements. Organizations should carefully evaluate the checklist settings and give them considerable weight, then make any changes necessary to adapt the settings to the organization's environment, requirements, policies, and security objectives. All deviations from the settings in the checklist should be documented for future reference." [36] After the completion of this step, a system with all corresponding documentation should be available for the Assess step, which is not covered in this document (NIST SP 800–53A). This completes the engineering process in the NIST RMF, as we progress towards developing a security policy for mobile devices.

Above, we have defined a security policy, security controls and the engineering processes. Using this framework we start developing a security

policy for mobile devices, or specifically what unique security requirements exist for mobile devices. The strategic goals, objective, and priorities for a mobile device have already been listed earlier in this document. So now we must move onto the strategic goal for a DoD security policy, prior to collecting all applicable laws, directives, and policy guidance.

D. DOD SECURITY POLICIES

1. Department of Defense (DoD) Security Policy

The DoD security policies primarily address the confidentiality of national security information. Specifically, the main focus of DoD information security policy is the classified National Security Information (NSI) which is categorized into three different hierarchical levels of classifications. The levels, in order of increasing information sensitivity, are Confidential, Secret, and Top Secret. [41] The lowest level is unclassified, the highest level being Top Secret. The information sensitivity level below the classified levels is Unclassified. In this structure, information may flow up from all levels to the levels above, but information may not flow down [42]. In this way, the DoD is essentially a confidentiality model implementing Mandatory Access Control (MAC) and is well modeled by the Bell/LaPadula security model.

However, the vast majority of DoD business is conducted in the unclassified domain and much of this information must also be protected. The unclassified domain of information is one of the areas we are examining for processing on mobile devices. The protection of unclassified information is governed by a simple policy, which makes the distinction among Controlled Unclassified Information (CUI) information and other minor forms of unclassified information. CUI is defined in the Department of Defense Instruction (DoDI) 5200.01 as follows:

> A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Reference (e), but is pertinent to the national interests of the United States or to the important interests of entities outside the

> Federal Government and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. [43]

This is information such as privacy information, health information, proprietary information, and any information, determined to be sensitive in nature such as information, which, if observed by the enemy, would jeopardize Operations Security (OPSEC) of a given mission.

The information flow for unclassified information is fairly simple. Unclassified information may not flow to the public domain with the only exception being once it is deemed officially releasable by Public Affairs. CUI is additionally restricted to only being releasable on a “need to know” basis. This means CUI must be properly labeled and additional access controls must be used which ensure it is only accessible to those with a “need to know” the information. Therefore, unclassified information and specifically CUI is governed by a Discretionary Access Control (DAC) as the release of this information is left to the judgment of individual entities who are responsible for controlling the release of the information to those who are authorized to have the information, basing the decision on “need to know” rather than assigned security labels.

For a DoD policy, attention must also be paid to the integrity and availability of the information system and its data. The integrity portion of the security policy “will need to assure the accuracy and reliability of the information and device, and prevent any unauthorized modifications” [44]. The goal of the integrity portion of the security policy is to protect the high integrity system functions, device applications, and data from the lower integrity applications, code, and data. While the goal of the availability portion of the security policy will be to ensure “reliable and timely access to data and resources to authorized individuals and applications” [44]. The levels of integrity and availability for information stored by the device are as defined by FIPS 199, discussed earlier in this document. These levels from FIPS 199 will lead to the security controls selected to assure integrity and availability of the system.

2. Executive, Federal, and Defense Organizational Policy

The goal of this section is to begin our security policy objects review with organizational policies. A higher-level organizational policy specifies what is to be achieved by proper design and use of a computing system. For this document, the organizational policies will come from existing Executive, Federal, and Department of Defense (DoD) Information Assurance (IA) policies. From this collection of policies, we will select a subset based on their applicability to the unique aspects of mobile devices. This selection process will include analysis of these existing policies to determine if they require modification to accommodate mobile devices. The initial list of policies analyzed based on potential content unique to mobile devices is as follows:

- ASD(NII)/DoD CIO Memo DoD guidance on protecting personally Identifiable Information (PII) [45]
- ASN(NII)/DoD CIO Memo Protection of Sensitive DoD Data at Rest on Portable Computing Devices [46]
- CNSSAM IA 1–10 Reducing Risk of Removable Media in National Security Systems (NSS) [47]
- CNSSI-1253 Security Categorization and Control Selection for National Security [48]
- CNSSI-4007 Communications Security (COMSEC) Utility Program [49]
- CNSSI-5000 Guidelines for VOIP Computer Telephony [50]
- CNSSI-5002 National Information Assurance Instruction for Computerized Telephone Systems [51]
- CNSSP-1 National Policy for Safeguarding and Control of COMSEC Material [52]
- CNSSP-14 National Policy Governing the Release of IA Products/Services [53]
- CNSSP-17 National Information Assurance Policy on Wireless Capabilities [54]

- CNSSP-25 National Policy for Public-Key Infrastructure (PKI) in NSS [55]
- Common Criteria [56]
- DoD CIO G&PM Acquiring Commercial Software [57]
- DoDI 8500.2 Information Assurance Implementation [12]
- DoDD 4630.05 Interoperability and Supportability of IT and NSS [58]
- DoDD 8100.02 Use of Commercial Wireless Devices, Services, and Tech in the DoD GIG [59]
- DoDI 5200.01 DoD Information Security Program and Protection of Sensitive Compartmented Information [43]
- DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems [60]
- DoDI 8420.01 Commercial Wireless Local Area Network (WLAN) Devices, Systems, and Technologies [61]
- DoDI 8523.01 Communication Security (COMSEC) [62]
- DoDI 8552.01 Use of Mobile Code Technologies in DoD Information Systems [63]
- DTM-08–003 The next generation of Common Access Card (CAC) Implementation Guidance [64]
- Executive Order 13556 [65]
- FIPS PUB 140–2 Security Requirements for Cryptographic Modules [66]
- FIPS PUB 199 Standards for Security Categorization of Federal Info and Info Systems [38]
- FIPS 200 Minimum Security Requirements for Federal Information Systems [39]
- M-05–24 Implementation of HSPD-12 [67]
- NACSI-6002 Nat'l COMSEC Instruction Protection of Gov't Contractor Telecoms [68]

- NSTISSP-101 National Policy on Security Voice Communications [69]
- NIST SP 800–53 R4 Recommended Security Controls for Federal Information Systems [33]
- NIST SP 800–60 Guide for Mapping Types of Info and Info systems to Security Categories [37]
- NIST SP 800–61 Rev 2 Computer Security Incident Handling Guide [70]
- NIST SP 800–153 Guidelines for Securing Wireless Local Area networks [71]

The first step of our policy analysis was determining the actual applicability of these policies to the unique aspects of mobility. This was accomplished by comparing the content of these potentially unique policies to the functional requirements and security context for mobile devices. The unique aspects and policies derived from this analysis are as follows:

- High concentrations of PII—Mobile devices store a massive amount of PII, beyond what is currently stored on standard information system deployed today because of their function as a personal digital assistant/organizer. Examples of information that is currently stored on these devices include biological information, Social Security Number (SSN), driver's license information, account numbers, current location, and contact information (like mother's maiden name). The policy that focused on this unique aspect of mobility was the ASD(NII)/DoD CIO Memo DoD guidance on PII.
- Based on Removable Media—Mobile devices are built upon removable media, and are often categorized as removable media in current security policies. The reason for this categorization is because current policies are written for immobile or docked

technologies. The policy that focused on this unique aspect of mobility was the CNSSAM IA 1–10 Reducing Risk of Removable Media in NSS.

- Voice Over Internet Protocol (VOIP)—Mobile devices will more than likely have a VOIP client installed as an application. Even if a VOIP client is not installed, mobile devices are transitioning to 4G communication technologies, which are based on VOIP infrastructures [72]. The policies that focused on this unique aspect of mobility were the DoDI 8500.2 (ECVI) and CNSSI-5000.
- PKI and Digital Signatures–Mobile devices may need to utilize the PKI infrastructure in a different method than currently deployed solutions. The entire process of building and configuring the mobile device (from manufacturing, to the ISP, to the user authentication) may all enable digital signing and authentication differently with different roots of trust. The policies that focused on this unique aspect of mobility were the DoDI 8500.2 (DCBP and IATS), CNSSP-25, DTM-08–003, and M-05–24.
- Mobile Code and Application Stores—Mobile devices heavily utilize cloud service providers that employ mobile code through a browser or mobile application. In addition to mobile code, the mobile application store will deploy and update applications in a much more rapid manner than currently deployed information systems. An additional difference with mobile devices is the nature of permissions granted to applications. Each application may have its own granular set privileges over data and sensor access on the device (like user accounts) instead of the privileges of the account that installed the application. The policies that focused on this unique aspect of mobility were the DoDD 8100.02, DoDI 8500.2

(DCMC, DCSQ, DCSR, ECCD, ECLP, ECML, ECPA, IAAC, and VIVM) and DoDI 8552.01.

- Wireless Access—Mobile devices will connect to a variety of different wireless providers, with the primary access being cellular, which does not provide the typical network boundary defenses. The ownership and network defenses of these wireless providers will differ among the DoD, commercial, public, and other mobile devices (mesh networking). An additional difference is that mobile device may also act as a wireless network access point to other devices as well. The policies that focused on this unique aspect of mobility were the DoDI 8420.01, DoDI 8500.2 (COEB, DCID, EBBD, EBCR, EBPW, ECIC, ECND, and ECWN), and NIST SP800–153.

- Outsourcing of IA and Incident Response—Mobile devices will receive transmit, and store information across a wider variety of commercial and DoD service providers because of the variety of network connection, cloud services, and mobile applications. This means a larger coordination effort whenever an incident occurs. The policy that focused on this unique aspect of mobility was the 8500.2 (DCDS and VIIR).

- Previously Assumed Physical Protection Mechanism—Mobile devices will not have the assumed physical protection mechanisms that are currently in place for docked/stationary computing devices. This is a defense in depth mechanism that will be lost, and may have to be recognized and account for in a different manner. This also occurred with the transition to laptop and notebook computers, which required an emphasis on whole disk encryption. The policy that focused on this unique aspect of mobility was the 8500.2 (PEs).

It is important to note that there are other areas that will need to be considered when developing a complete security policy for mobile devices that are not covered in this thesis. Such areas include the security policies for cloud service providers, ISPs, and mobile controlled COMSEC equipment. It is also important to note that there are additional security policies that apply to mobile devices beyond the ones selected. Since the applicability would not differ greatly from currently deployed information systems, they are also not covered in this thesis.

The next step of our policy analysis was to determine if any modifications to current organizational security policies are required to support mobile devices. This analysis was performed using our definition of organizational security policies; they describe the resource that needs to be protected with the corresponding level of protection required. After analyzing the policies listed above, the answer (in general) was that no modifications are required. Most organizational policies stated a specific Information Assurance (IA) requirement with corresponding responsibilities for each agency to implement. Therefore, the need for modifications to the organizational policies is minimal. However, the chances of revisions being necessary increased as specific technological requirements were included with the organizational policy. Example of such revisions or updates that may be required are:

- Citing specific technological solutions in organizational security policies– A number of policies, such as CNSSP-25, require CAC authentication to the DoD PKI, which is a specific form of two-factor authentication. The earlier CAC requires a hard connection that may not conform to the way mobile devices are currently being utilized. Though there are policies, such as DTM-08–003, that call for the next generation of CAC which may resolve these concerns by enabling wireless authentication. Another option being considered in the updated FIPS 201–2 could include derived

credentials, which stores credentials on a tiny microSD card that can fit inside mobile devices [73].

- Mobile devices and PII –As stated earlier, mobile devices will store and process massive amounts of PII. Current policies only allow mobile devices to store this information by exception, such as ASD(NII)/DoD CIO on PII. Even with this possible exception, such devices are required to be stored in a "protected workplace" that meets the physical and environment controls for confidentiality level of sensitive. There is a high probability that these devices will need to be used outside of these "protected workplaces," so these policies will likely need to be updated to reflect technical vice physical protections.
- Categorizing Mobile Devices as Removable Media– Currently there are policies, such as CNSSAM IA 1–10, that categorize mobile devices as removable media (such as Compact Disks (CDs), Digital Video Disks (DVDs), thumb drives, Universal Serial Bus (USB) storage). When mobile devices are placed in this category in policies, they end up having inappropriate security restrictions placed on the mobile devices. When categorized this way, the appropriate controls are not applied to secure such devices.
- VOIP and Mobile Devices in Secure Spaces– Currently mobile devices, especially using VOIP, are not permitted in accordance to policy since they cannot meet the current requirements. This is due to the fact that mobile devices not meet the security requirements, such as those for voice instruments described in CNSS-5000. In order to utilize mobile device in secured spaces, a new set of security requirements and mechanisms may be necessary. This could be an area of future research.

- Mobile Code from Trusted DoD Sources– The ownership of a BYOD mobile devices, and personality, would have to be determined in order to analyze the level of policy applicability. If it is determined that the whole device, or information system, is owned and controlled by the DoD, then policies like DoDI 5200.44 would apply for mobile code. This would mean that mobile code used on other personalities, such as personal, may be restricted to trusted DoD sources defeating a major functional purpose of BYOD. If this is the case, the policy may need to be updated with restrictions of information flow vice prohibition.
- Environmental Controls—The DoDI 8420.01 states that Access Points (APs) used in unclassified WLANs should not be installed in unprotected environments due to an increased risk of tampering and/or theft. Mobile devices are now on demand access points that are not always located in a protected environment, for example a user's home.
- Personal Use of services on DoD devices– Currently there are policies, such as DoDI 8500.2, that restrict personal use of services on DoD devices. If it is determined that BYOD mobile devices are owned and controlled by the DoD, than current policies restrict use of personal services such as VOIP (DoDI 8500.2 ECVI-1). This may mean that that current policies may need to be updated to reflect restrictions of information flow vice prohibition.

We have now analyzed the organizational security policies in regards to the unique aspects of mobility. In summary, a small number of the current organizational policies affect the unique aspects of a mobile device. This is due to these policies being rightfully technology independent. Of that small number of policies that affect the unique aspects of mobility, an even smaller portion

would have to be modified to accommodate the mobile devices discussed in this document. With this analysis completed, we move down to the next level of security policy to security controls.

3. Security Controls

Security controls are put in place to enforce organizational objectives for information systems while remaining device independent. At the security control level, we chose to address the DoD 8500.2 controls above and focus on the NIST controls documented in the NIST SP 800.53. Although the DoDI 8500.2 controls exist, they are being updated to reflect the NIST SP 800.53 controls. Of the NIST 800.53 revisions, we chose revision 4 because it is the most recent version and updated to include some mobility issues.

As noted earlier there are a wide variety of controls listed in NIST SP 800.53. However, not all of the controls are relevant or require special consideration when applying them to mobile devices. We organize the mobile device aspects of security controls into two categories in respect to our previously listed use cases. These categories are “mobile interesting” and “mobile unique.” Mobile interesting controls are addressed in the NIST SP 800.53, but require modification or special consideration when applying them to mobile devices as compared to more traditional information systems. Mobile unique controls are ones that we believe must be added to the NIST security controls baseline to address mobile devices, our use cases, or DoD security policy objectives. To begin our categorization of these controls, we will start with the security control families (e.g., Access Control and Configuration Management). From these control families, we will continue to categorize these controls based on the family identifier and control number (e.g., AC-2 and CM-2) [33]. Using this process of categorization, we will begin with documenting mobile interesting security controls:

a. Family: Access Control (AC) [33]

The “access control” family of controls addresses account management, access to systems, and access to information. The mobile interesting portion of this family is where the mobile device supports multiple personalities. Each personality may implement access control differently. As such, the device should support all the implementations without allowing them to conflict with each other. With personalities, the user is the same person accessing each personality, but account management may be handled differently across the personalities. For example, the employer personality may require two factor authentication. Whereas the user’s personality may require a four-digit pin. Some of the specific control issues to consider are:

- AC-2 Account Management [33]: Accounts will not be system specific but personality specific. As such, there must be a way for an administrator to terminate account access even in the BYOD scenario where the government does not own the device. Simply put how does one provision and un-provision the DoD personality access?
- AC-4 Information Flow Enforcement [33]: Enforcing the flow of information is essential to all our use cases for mobile devices. Mobile devices should allow one to share information with the user who is central to all the personalities without allowing unapproved information into a separate COI. On the other hand, as is the case for use cases involving the camera and GPS for instance, the personalities share the use of the mobile device resources/capabilities. Therefore, these resources must be able to properly enforce not only the flow of personality provided information but also the flow of information generated by the resource. For instance, in the battlefield, a

picture taken for intelligence purposes should not be sent automatically to the user's Google+ account.

- AC-4 Information Flow Enforcement [33]: The information flow among applications, sensors, and wide array of wireless networks is unique to mobile devices. An example of such a unique requirement is the precedence of access to sensors; for example when two domains want continuous access to a sensor to perform a function, which domain obtains access and for how long? Another example would be the sensitivity of information as perceoeved by different personalities; when an application is pulling sensitive (e.g., CUI) sensor information in a government domain, should a personal domain be allowed to pull the same sensor information concurrently or even a second later? All of these questions and more would have to be addressed to securely enable BYOD and multiple personality mobile device.
- AC-7 Unsuccessful Logon Attempts [33]: Mobile devices are unique in that they can be easily left in areas in which they are unprotected and therefore easily fallen to the wrong hands. As is the case, this means unsuccessful logon attempts could be a good indication of compromise. Therefore, rather than simply locking the device, it may be wise to zeroize the device when a number of unsuccessful logon attempts occur. However, this functionality should be personality dependent. The DoD personality may want to be zeroized after 3 unsuccessful attempts, but maybe another personality may not require zeroization at all. Therefore, only the appropriate personality should be zeroized at the appropriate time, while leaving high availability or emergency services available.

- AC-8 System Use Notification [33]: In the mobile device BYOD use cases, it is not likely the DoD would be able to justify monitoring all activity on a personal device. Additionally, system notification is system centric whereas on a mobile device, maybe access control focus should be on the DoD information stored on the device.
- AC-16: Hardware Root of Trust [33]: "Mobile devices are not capable of providing strong security assurances to end users and organizations; these devices lack the hardware-based roots of trust that are increasingly built into laptops and other types of hosts." [74] This hardware-based root of trust may be essential to providing remote COIs (owners) the ability to verify the state of the device, either prior to placing a personality on it or after for monitoring.

b. Family: Audit and Accountability (AU) [33]

The audit and accountability family of controls address the data, policy, procedures and processes required for an information system to record security relevant activities with individual accountability. For mobile devices, this would most likely occur through a MDM solution. The mobile interesting portions of this family of controls focuses on the mobile device's multiple personalities, increased number sensors, numerous communication infrastructure, hardware limitations, and high availability needs (such as military radio and emergency phone calls). Specifically the mobile interesting controls are:

- AU-2 AUDIT EVENTS [33]: Since there are potential security conflicts occur when several personalities access sensor information at the same time (detailed in the security misuse cases), organization-defined auditable events should include when multiple personalities access sensors or the communication infrastructure at the same time. This would

be used to help detect when sensitive information is being provided to the wrong domain or when a domain is attempting to communicate using a prohibited medium. It would also be useful for organization-defined auditable events to include when the device is being used outside of its typical geographical area (such as GPS, compass, or barometric sensors) to detect possible theft or misuse, since the probability of this occurrence will increase with mobile devices.

- AU-3 AUDIT CONTENT [33]: Mobile devices are able to utilize a wide variety of additional sensor information that could help increase the security posture of these devices. One such sensor is GPS, which could be utilized in researching or resolving security relevant events. To achieve this, audit data should include where the device is being used when an auditing event occurs, while recording the communication interface being utilized at the time of the event (such as GPS, compass, or barometric sensors).
- AU-4 AUDIT STORAGE CAPACITY [33]: Mobile devices are by nature resource limited. As such, the storage capacity of these devices is limited. It would not take a long time to fill the device with logs hindering functionality, creating a denial of service. Since the device requires connectivity for many of its functional activities, this connectivity should be used to store audit logs via MDM solution. The device could be the contingent audit storage location when connectivity fails. As such, the logs should be protected accordingly when being transmitted across networks of a various levels of confidentiality.

- AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING [33]: Mobile devices will contain information from all aspects of the user's life. This could cause some complexities when audit logs contain data from different personal and work related organizations. One such complexity would be the responsibility and authority of a single organization collecting all of this log information for review, analysis, and reporting. One example could be private log data, such as browsing history on non-work related personalities. The user would not want private data being reported for review and analysis by the employer. A possible way of implementing this protection could be a policy that adjudicates other log policies among personalities.
- AU-8 TIME STAMPS [33]: Mobile devices with multiple personalities could run into a situation where each personality obtains its time from a different organizationally approved source. This could cause complexities when there is a review of audit logs to determine an event's actual time of occurrence. This could be a potential area of future research.
- AU-5 RESPONSE TO AUDIT PROCESSING FAILURES [33]: Mobile devices will provide functionality with high availability needs, such as military radios and emergency phone calls. As such, these functions with high availability needs should stay functional when audit failures occur. To achieve this, the device could possibly enter a degraded operational mode for functions with lower availability needs. If such a mitigation does not occur, there exists the possibility of an attack on a mobile device when the logs are

purposefully filled up to create a denial of service. Policies and procedures for handling this situation could be an area of future research.

- AU-13 MONITORING FOR INFORMATION DISCLOSURE [33]: As discussed earlier in this document, mobile devices will have sensors that communicate with applications that can automatically post information collected to cloud services (e.g., GPS location or photographs to foursquare [75] or facebook [76]). This could have significant security ramifications, if sensor information is being collected by a sensitive domain, while other domains (e.g., personal) are still recording and posting that same information publicly. To detect such actions, the organization should employ an automated mechanism for monitoring if sensor information from mobile devices is being disclosed in an unauthorized manner to open source sites, for example foursquare [75].
- AU-16 CROSS-ORGANIZATIONAL AUDITING [33]: Mobile devices could have applications within a personality that transmit information outside of the organization that deployed it. The organization should audit information for such information, to detect when sensitive information is being improperly provided to an organization without proper authorization. Mobile devices could have also applications within a personality that communicate with other applications in other personalities. All such actions should be audited.

c. Family: Configuration Management (CM) [33]

The configuration management family of controls addresses how the configuration of the information system is known and subsequently controlled. For mobile devices, this is performed through Mobile Device

Management (MDM) solutions deployed by each organization, or COI. Considering the fact that mobile devices are intended to be configured and altered by the user according to their perceived needs, there are many interesting aspects to the application of CM. Policy may need to be created that deal with the ownership and management of the MDM services for the BYOD use-case scenario.

- CM-2 Baseline Configuration [33]: In a BYOD scenario there will have to be specific MDM solutions for each configuration authorized for access to the system and there would have to be a way for the organization to ensure the device initially and routinely meets these requirements. This would be a major part of the assumptions, which would have to be made about the security capabilities of the device to enforce our multiple personality scenarios.
- CM-3 Configuration Change Control [33]: In this control, the organization is expected to specify what changes must be addressed by the configuration control process. For a BYOD mobile device, could the organization have an expectation of controlling a portion of the configuration within other personalities, how much of the configuration could be device-specific versus personality specific?
- CM-5 Access Control for Change [33]: This control requires the organization to control physical and logical access associated with changes to the information system. Here again it is interesting how the control should be implemented considering the BYOD and/or multiple use case scenarios. The organization should be assured of certain configurations which include the required assumptions for implementing their information protection policies, but how much can the

organization control a BYOD device, and how much should the organization allow the user to change configuration of the other personalities?

- CM-10 Software Usage Restrictions [33]: In a multiple personality use case or particularly with a BYOD use case, the implementation of this control must consider the personal use of the device and how much the organization can and should restrict the user from doing with their personality and/or their own device.
- CM-11 User Installed Software [33]: Particularly with mobile devices which rely on an "application market" concept for provisioning the device, users may be able to download and install software for all personalities. In our use cases where the individual has a personal personality on the device, the intent is to allow the user to install any application they find in the commercial market place. In this use case, the user could install malware or application normally deemed inappropriate for use on an information system associated with the DoD.

d. Family: Incident Response (IR)

The Incident Response (IR) family of controls address the policy, procedures and processes required to prepare for and respond to security incidents involving an information system. The mobile interesting portions of this family of controls focuses on the mobile device's cloud services and mobile carrier access. Specifically the mobile interesting controls are:

- IR-4 and IR-7 INCIDENT HANDLING [33]: Mobile devices will be heavily reliant on mobile carriers and cloud service providers for storing, processing, and transmitting information. Because of this reliance, organizations using

mobile devices will need to actively coordinate with mobile carriers and cloud service providers in planning and responding to incidents. This coordination should include sharing incident response capabilities, protection mechanism, and points of contact. A firm understanding should be in place among these partners to understand where information transmission, storage, and processing is taking place to help identify information systems or system components that may be subsequently contaminated. Organizations would also benefit from coordinating with mobile carriers and cloud service providers to correlate and share incident information to achieve a cross organization perspective on incident awareness.

e. Family: Media Protection (MP)

The Media Protection (MP) family of controls address the policy, procedures and processes required to protect digital and non-digital media. The mobile interesting portions of this family of controls focuses on the mobile device's storage, removable storage, and personalities.

- MP-4 MEDIA STORAGE and MP-5 MEDIA TRANSPORT [33]: Mobile devices will store information on media that would typically have additional layers of physical protection. These layers of physical protection are not available for mobile devices because they will be transported outside of controlled areas frequently. To help protect against the risk of sensitive information being stored on digital media while transported outside of controlled areas, cryptographic mechanisms could be used to provide confidentiality and integrity protections.

- MP-6 MEDIA SANITIZATION [33]: Mobile devices will access and store information at a CUI level and higher. As such, they present a risk to these protected information systems that processes CUI. The first way this risk is incurred is when the mobile devices are connecting to CUI information systems directly from the vendor or after being directly exposed to the cyber threats on the Internet. To protect against this risk, the mobile devices should be sanitized in a non-destructive manner prior to creating new CUI or “higher” personality or when connecting to a new CUI or higher information systems, as policy permits. The organization should also have the capability to remotely wipe individual files or entire personalities when the device is stolen, compromised, or the user no longer requires that personality.
- MP-7 MEDIA USE [33]: Mobile devices with different personalities and classification levels may have access to removable media. As such, these personalities may require protection mechanisms to limit the access of the information stored on the media to a specific CUI or to other personalities and applications. The mobile device should support such separation, through mechanisms such as cryptography or access control lists managed and enforced by the underlying infrastructure of the device. When a personality is no longer required, or no longer requires removable media access, the removable media should have the capability of being sanitized.
- MP-8 MEDIA DOWNGRADING [33]: Mobile devices will have personalities that store information with different levels of classification, such as CUI or PII, that may come and go

with time. To accommodate these role changes, the mobile device should have a downgrading process to include the removal of a personality with CUI or data and programs with "higher" information. There may also be times that information, from items such as sensors, is obtained in a personality at a CUI or higher level of sensitivity. The mobile device should have the capability to downgrade the sensitivity of such information in accordance to an organizationally defined policy.

f. Family: Identification and Authentication (IA) [33]

The Identification and Authentication (IA) family of controls address the data, policy, procedures and processes required for supplying and verifying identification information for the information system to make proper authorization decisions. The mobile interesting portions of this family of controls focuses on the mobile device's context aware functionality, wearable computing, mesh networking, and mobile carrier access. Specifically the mobile interesting controls are:

- IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) [33]: Certain policies that made sense for desktop computers may not make sense for mobile devices. We propose that pin and passcodes are one of those policies for mobile devices. Forcing a pin or passcode prior to obtaining information from a mobile device will hinder functional use cases, or cause potential dangerous security exceptions (as documented earlier in "alerting terrorists of U.S. friendly forces"). As such, we would want to still authenticate the user to the device, but potentially use a different combination of something you have, know, and are. This is could be made possible

because the device has the capability of context awareness with additional detailed information on its user. In relation to authorization, identification on one personality should not necessarily permit access to another personality unless agreed upon by security policies of the COIs involved. Describing and implementing this policy and functionality is a subject further research.

- IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION [33]: In accordance to our functional use cases, mobile devices could communicate with other mobile devices to create a mesh network. Mobile devices will also communicate with other sensor devices to collect data about the user and outside world. This raises the question of identification and authentication of these devices to each other. This means that organizations will have to define the devices requiring unique device-to-device identification and authentication. This will require further analysis, and could be an area of future research.
- IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) [33]: Currently most patching of the mobile devices is performed through privileged access provided by mobile service providers. This may need to be addressed through a strong partnership between the COIs and the mobile service providers to uniquely identify and authenticate such access. This could be an area of future research.
- IA-10 ADAPTIVE IDENTIFICATION AND AUTHENTICATION [33]: Adversaries may compromise individual authentication mechanisms and subsequently

attempt to impersonate legitimate users. This situation can potentially occur with any authentication mechanisms employed by organizations. To address this threat, organizations may employ specific techniques/mechanisms and establish protocols to assess suspicious behavior. For mobile devices, such a suspicious behavior could be identified when information/service are accessed at unusual times and locations. In these situations, when certain pre-established conditions or triggers occur, organizations can require selected individuals to provide additional authentication information. Again, this is a topic for future research.

g. Family: System and Communication Protection Control (SC) [33]

The System and Communication protection (SC) control family focuses on system security and the protection of information in transit. For a mobile device, what is most interesting about this control is the nature of how the mobile device may communicate to the associated communities of interest. One must consider how to protect confidentiality and integrity of communication when the networking layer is owned and operated by a third party. This forces the mobile device in our use cases to implement a context aware security policy.

- SC-6 RESOURCE AVAILABILITY [33]: Mobile devices may be the primary communication medium for their users to the outside world. As such, they may need a higher level of assurance for availability than their notebook or desktop counterpart. This can be demonstrated with functions that were previously performed over radio on the battlefield or emergency phone calls performed over analog signal. Additional security protections such as Denial of Service

(DoS) prevention, priority of communication services, and higher assurance of communication services/application may be required. As we progress towards 4G/VOIP, where DoS attacks and loss of availability may become more prevalent, this higher assurance requirement of availability may become self-evident. Some example functional security requirements that could be included are redundancy in communication protocols and services; or a minimum set of communication applications available upon certain levels of device failure.

- SC-7 BOUNDAY PROTECTION [33]: Mobile devices use many different networks to communicate. Many of these networks may be owned by third party commercial or private parties. As such, these networks may not afford the protections offered by the organizational (COI managed) network. Therefore, one must consider whether or not a mobile device requires boundary protection. For instance, a mobile device using an airport hot spot service should be able to implement some sort of self boundary protection. However, it may also restrict network access on a given personality unless the device has implemented a VPN with the associated COI.

- SC-10 NETWORK DISCONNECT [33]: Typically network disconnect makes sense for making sure secure communication are not left open for potential exploitation and to protect against resource consumption. However, one of the assumptions of the mobile devices is that they are “always on.” Due to these assumptions, there are multiple reasons why one may want to keep communications open to a mobile device. For instance, there may be situations where

long term collaboration is required such as for a teleconferencing or team communication during a mission. In the form of unintentional network disconnects, future research, related to the information transport layer, should be considered for the deployment of mobile devices on the battlefield as TCP-IP may not be the best choice for noisy, burst heavy, and high-latency environments.

- SC-11 Trusted Path [33]: An additional enhancement might be needed to protect against the increased probability of the mobile device being swapped for a similar mobile device that steals the users' credentials. This could be accomplished by the device authenticating to the user (eg hardware based certificate or picture on login screen). Along the same lines, a "trusted path" might be required. This would be enabled to provide assurance that one is talking to the appropriate device, OS, COI, or application.
- SC-15 COLLABORATIVE COMPUTING DEVICES [33]: Context awareness can provide security features not previously possible. An example of such a use cases would be included in collaborative computing devices control, such as disabling / removal functionality in secure work areas. An example of such a collaborative computing device being restricted by context awareness would be turning off a camera. Additionally consideration must be given for the privacy of the individual especially for a BYOD use case. The expectation is the mobile device is always near the owner. Therefore, remotely activated collaboration aspects of a mobile device will have to be considered very closely.

- SC-28 PROTECTION OF INFORMATION AT REST [33]: Mobile devices are particularly vulnerable to theft, loss, or physical tampering/exploitation. For this reason, mobile devices in particular should protect information at rest. Additionally, it would be useful to implement some sort of additional protection measure to wipe the information either remotely or when an authorized attempt is made to access the device such as it is written in the 8th enhancement to the control MP-6 MEDIAN SANITIZATION.
- SC-40 OPERATIONS SECURITY [33]: There are several OPSEC consideration related to mobile devices that should be evaluated. As is the case with a laptop, when in public the screen for a mobile device can be read by a passerby. When used for voice communications, someone close by can listen in on at least half the communication. Also, mobile devices can sometimes be left unattended with the device unlocked at least until the inactivity timeout. In these situations, it would be possible for someone to pick up the device and "look around" for information. Finally, the government has a tendency to purchase a certain "profile" device which could indicate to an "outsider" that the owner works for the DoD. Additionally, it is still common to allow complete strangers to use your mobile phone when they are in need. In these cases, they have open access to the phone and it is possible they could use this opportunity to access information they are not authorized to access. These situations must be considered and mitigations developed in order to address any opportunity for exploitation.
- SC-42 SENSOR DATA [33]: In a multiple personality environment there are two new considerations: First,

sensors may need to be restricted based on context and the COI required security policy. For instance, when the user enters a classified space, the camera must be disabled. Second, COIs may want to remotely control sensors on the mobile device, this access will have to be managed as the sensors are a shared resource.

- SC-43 USAGE RESTRICTIONS [33]: Many mobile devices allow the user to add additional storage via flash drive. Even in a BYOD use case, there will have to be restrictions on the use of such media in order to protect the trustworthiness of the platform. Other more simple uses must be addressed. As discussed earlier, what if someone asks to make a phone call with your mobile device? In these cases, it is not prudent to allow others to use the mobile device since they will have access to all the information on the phone.

h. Family: System and Information Integrity (SI) [33]

The System and Information Integrity (SI) family of controls assure the accuracy and reliability of the information and system, and prevent unauthorized modification**.** [44] The mobile interesting portions of this family of controls focuses on the personalities, COIs, resource limitations, and mobile carrier access. Specifically the mobile interesting controls are:

- SI-2 FLAW REMEDIATION [33]: Currently most operating system patching of the mobile devices is provided by mobile service carriers. This may need to be addressed through a strong partnership with mobile service carriers to allow patch distribution only upon the code/patch/change being signed by a government authority. One potential drawback of such a solution is a delay in software updates, leaving the updates of these devices lagging behind the commercial sector. Most

patches for applications are currently provided through an application store, which may or may not be owned by the organization that owns the personality or domain. This will also take strong partnerships and coordination among the developers, the COI(s) and the service carriers to ensure software updates are tested for security, effectiveness and potential side effects.

- SI-3 MALICIOUS CODE PROTECTION [33]: The deployment of malicious code protection will need to be carefully weighed against resource availability on the mobile device to ensure that the required protection is provided while leaving the device operational. Ideally malicious code protection would take place in the app stores, within each personality, as well as at a level below each personality (watching the watcher). For the layer below each personality, and other critical interfaces or privileged applications, malicious code protection may be required for detection of unauthorized commands. Unauthorized operating system commands include, for example, commands that access kernel functions from information system processes that are not trusted to initiate such commands, or commands for kernel functions that are suspicious even though commands of that type are reasonable for processes to initiate.

- SI-4 INFORMATION SYSTEM MONITORING. EXTERNAL [33]: Currently most external interfaces for mobile devices are managed by service carriers or providers. As such, different COI's may require these boundaries to be monitored. This may need to be addressed through a strong partnership with service carriers or access providers, to include who owns the results from monitoring activities.

Another option could be VPNs back to the organization's, or COI's, network defense suite. Once these options are decided, there will need to be a determination on how private user data within their private personality will be handled, while monitoring, to ensure that there is no violation of privacy. This may require current policies to be updated.

- SI-4 INFORMATION SYSTEM MONITORING [33]: INTERNAL: For internal system monitoring as mentioned earlier for malicious code protection, the same carefully weighing of options would also need to take place. For example, the decision on which products would belong in each personality and "below" each personality (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). It would be useful, if resources allow, to integrate intrusion detection tools into access control and flow control mechanisms below the personality. This could allow for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination. For example, if a personality is deemed a threat, it could be isolated completely from the other personalities, network interfaces, and mobile device.
- SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY [33]: Since mobile devices will allow execution of code obtained from various sources, including possibly commercial application stores, the software will need to be confined virtually to the deploying organization's personality. This could be accomplished through multiple domains on the device. Roots of trust should also be used since information owners, COIs, will have to rely on remote mechanism to

ensure software, firmware, and information integrity. Along with the roots of trust, there should also exist certificate chains to help further establish a chain of trust among the user, applications, OS, Device and COIs. The architecture, organization, management/application and distribution of such certificates is an area of future research.

- SI-14 NON-PERSISTENCE [33]: It may be useful to mitigate against "advanced persistent threats" [33] by significantly reducing the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete cyber-attacks. This could be done for highly sensitive personalities by making them non-persistent. This could possibly be accomplished through domain virtualization and automatic restoration of the personality when needed.

i. Family: Personnel Security (PS) [33]

The Personnel Security (PS) family of controls covers personnel actions to include screening personnel and access agreements. Here again the focus appears to be on system access versus access to information. For instance:

- PS-3 Personnel Screening [33]: This control focuses on allowing access to an information system. However, the main concern is access to information. In the BYOD use case, the individual will already have access to their own information and physical system. If other COIs vet their members prior to granting them access to that community's information, that should be a precursor to instantiating those COI's presence on the mobile device.

- PS-4 Personnel Termination [33]: There must be provision for removing information or access to the information from the mobile device even if the device is personally owned with a DoD personality. In our use cases where multiple personalities are accessed on the device, the DoD COIs must have the ability to ensure that their personalities are erasable from the device and must have a way of ensuring that that erasure has occurred.
- PS-6 Access Agreements [33]: Access agreements must now consider the multi-personality environment. Particularly, the DoD must consider what activities are not allowed on a multiple personality device. For instance, if on my personal personality I choose to visit a gambling site the government would normally consider an inappropriate use of resources, should the government block this activity? Furthermore, in the case of a BYOD mobile device, what are the expectations for behavior and what are the limits of what the government or any other organization should control? What about political activities associated with the device, what should the limitations be in these cases?

j. Mobile Unique Security Controls:

NIST has already recognized some unique challenges created by mobile devices. On the latest draft of NIST SP 800–53 revision 4, at least the following exist as controls specifically meant for application to mobile devices:

- AC-19 ACCESS CONTROL FOR MOBILE DEVICES [33]:– This control addresses how an organization should control access of mobile devices to organizational information systems to include usage restrictions. This control also

addresses supporting access control on the device through either full service or container-based encryption

- AC-7 (2) UNSUCCESSFUL LOGON ATTEMPTS | PURGE / WIPE MOBILE DEVICE [33]: This enhancement for AC-7 specifically addresses purging mobile devices when the password is entered incorrectly a defined number of times. This could be very useful for mobile devices since they can be easily lost or stolen due to their mobile nature.
- MP-6 (8) MEDIA SANITIZATION | REMOTE PURGING / WIPING OF INFORMATION [33]: This control is similar to the previous one in that the potential situation is recognized where a mobile device could be lost or stolen. In this situation, it may be best to protect confidentiality by remotely purging the information stored on the device. In a multiple personality environment one would have to consider whether all personalities should be erased with one command or single personalities based on COI controlled implementations.
- SC-7 BOUNDARY PROTECTION [33]: Considering the same situation as noted in MP-6 where a mobile device is either lost or stolen, not only should there be a functionality to purge resident information but it would also be useful to ban the device from access to the COI(s) in order to ensure boundary protection. Although, the device may require user I&A for access to the device, COI services are often set up to push data, alerts, and notifications on behalf of the user. This puts the device within some level of trusted network

boundary layer. Therefore, we may need to erase this relationship upon the realization that the device has been lost or stolen.

We also believe there is opportunity to provide additional controls specifically for the mobile devices. These controls are as follows:

- SC-XX Phone only Mode–Many of today's mobile devices are mobile phones. There are many cases where normal phone use assumes immediate access to the phone functionality usually without the requirement for Identification and Authentication (I&A). There is a NIST control which addresses part of this concern. AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION AND AUTHENTICATION [33] specifically addresses receiving calls without having to log in. But we need a way to specify that phone can be placed in a mode where all other functionality is restricted and only the phone functionality exists unless or until the user provides I&A. It is conceivable the mobile device owner may be solicited by a co-worker, friend, family member, or even a stranger to use the phone. In these cases, it would be prudent to lock out the temporary user from any other functionality. This control could also cover emergency call capabilities for mobile phones. This control would also be related to SC-24 FAIL IN KNOWN STATE [33], as you would not want one to be able to circumvent security implementations by forcing a system failure while it is in "phone only" mode. Note, this control would exclude VOIP applications existing within a particular personality. In these cases I&A would have to be established before using the VOIP capabilities.

- AC-XX Events Driven Access Control–Related to SC-42 SENSOR DATA [33] and SC-43 USAGE RISTRICTIONS [33], this control could be an enhancement to AC-3 ACCESS ENFORCEMENT [33]. This control would specify the ability to dynamically enforce access control lists, which could be altered dynamically, based on events or environmental context, as defined by the information flow enforcement.

We initially considered Bring Your Own Device (BYOD) as a mobile unique control for addition to the NIST catalog. However, we determined the existing controls already include this concept. AC-20, USE OF EXTERNAL INFORMATION SYSTEMS [33], covers all the elements we believe are required to control the use of personal devices.

Next we considered how the NIST controls cover our main concept of “multiple personalities” as separate security domains but with a “consolidated user experience.” After evaluating the controls, one could make the case that this concept is covered by multiple controls. For instance, the following controls could be added to a mobile device specific baseline to guide implementation of such a security construct:

- AC-4 [33], Information Flow Enforcement, covers the ability to control the flow of information. This is fundamental for maintaining the confidentiality and integrity of multiple personalities.
- AC-15 [33], Security Attributes, could be required to ensure information would be labeled to support access control.
- AC-19 [33], Access Control for Mobile Devices, determines usage restrictions for mobile devices and specifies full-service or container based encryption for confidentiality and integrity of information.

- AC-25 [33], Reference Monitor, there must be a functionality that exists at some lower level than the applications that enforces access control.
- SC-16 [33], Transmission of Security Attributes, allows information received form a particular Community of Interest (COI) to be labeled for a particular personality.
- SC-7 [33], Boundary Protection, is required to provide confidentiality of the personalities.
- SC-8 [33], Transmission Integrity and Confidentiality, would be used to maintain personality to COI confidentiality and integrity.
- SC-39 [33], Process Isolation, and SC-4 [33], Information in shared resources, are required to maintain confidentiality and integrity of personalities on the device.

However, we believe the NIST controls are written in a paradigm where an information system is implementing either a comparable multilevel security construct or a single level security construct. In our construct, we propose independent multiple level security domains. Therefore, we conclude the NIST mobile device baseline approach would not be explicit enough. A new control is required in order to create the correct context security levels. Otherwise, we believe this type of construct would be simply avoided as a possible implementation. Therefore, we propose our final mobile unique control:

SC-XY Multiple Independent Security Domains—This control would specify the need to ensure the information system can support the information flow of multiple independent security domains. It would address the requirement to determine an appropriate security flow and offer sub-controls or enhancements to cover the security implementations such as container-based encryption of the DoD personality, thin client implementation, or the requirement of a trusted process to act as a reference monitor [77]. This control would also

have to address the requirement for security attributes, specifically labeling versus non-labeled container-based access control implementations where the container is the personality. The related controls would be: SC-XX Phone only Mode, AC-XX Events Driven Access Control, AC-4 Information Flow Enforcement [33], AC-15 Security Attributes [33], AC-25 Reference Monitor [33], SC-16 transmission of security attributes [33], SC-7 Boundary Protection [33], SC-8 Transmission Integrity and Confidentiality [33], SC-39 Process Isolation [33], SC-4 Information in Shared Resources [33], and SC-42 Sensor Data [33].

4. System Specific Implementation

After addressing the IA controls, the next step would be analyzing the system specific implementation requirement. Our initial system specific implementation analysis started with determining all the applicable System Specific Implementation (SSI) policies. The original list of all system specific implementation policies was obtained from DISA, the National Security Agency (NSA), and NIST. The implementation policies applicable to mobile devices are:

- DISA Mobile Operating System Security Requirements Guide [78]
- DISA Mobile Device Management Security Requirements Matrix [79]
- DISA Mobile Applications Security Requirements Guide [80]
- DISA Mobile Policy Security Requirements Guide [81]
- DISA General Mobile Device (Non-enterprise Activated) STIG [82]
- NIST SP 800–124 Guidelines for Managing & Securing Mobile Devices in the Enterprise (Draft) [4]
- NIST Guidelines on Hardware-Rooted Security in Mobile Devices (Draft) [74]
- NSA Mobility Capability Package [83]

Given the time constraints and scope constraints for this thesis, DISA's Security Requirements Guides (SRGs) were the set of system specific implementation policies selected for inclusion into our security policy analysis. DISA SRGs represents an intermediate step between Information Assurance (IA) controls and mobile product-specific implementation information. Our analysis of the DISA SRGs determined that all comments associated with these documents have already been included in our IA control review. The only unique comment would apply to the SRGs would be an update or new element to accommodate the mobile devices discussed in this document. With that being said, the summary of the mobile interesting security policy topics that would have to be addressed from the SRGs and IA controls are:

- Provisioning and de-provisioning access to the DoD personality (AC-2) [33]
- Information flow among personalities, applications, sensors, and a wide array of wireless networks. Including the confidentiality, integrity, and auditing of such information and information flows. (AC-4) (AU-2) (MP-4) (MP-7) (SC-9) [33]
- Wiping/zeroizing a personality without affecting the other personalities on the device (AC-7) [33]
- DoD collecting, monitoring, and reporting personal activities on a non-DoD provisioned personality. This would include the ability of the DoD to restrict personal applications and services on a non-DoD provisioned personality. (AC-8) (CM-10) (AU-6) [33]
- Configuration Management of the device and personalities (device-specific versus personality specific) (CM-3) [33]
- Coordinating and Managing the official time source among personalities for security services such as auditing (AU-8) [33]

- Level of access provided to mobile service carriers for patching and servicing mobile devices. This would also include items such as mobile devices only accepting patches signed by the hosting organization. (IA-8) (SI-2) [33]
- Coordination of monitoring at external boundaries and the associated incident response activities. (IR-4)(IR-7)(SI-4) [33]
- Coordination of classifications/confidentiality levels and processes for regrading information among organizations. (MP-8) [33]
- Utilizing context awareness to increase the security posture of the mobile device. This could include sensor information for authentication, inclusion of sensor information (location) in security logs, or using sensor information, i.e., context awareness, to enable/disable services (such as camera in SCIF). (AU-3) (IA-2) (IA-8) [33]
- Planned deployment of security services (e.g., auditing, malicious code protection, Intrusion Prevention Systems (IPS), and monitoring software) on resource limited mobile devices. (AU-8) [33]
- Mobile applications with high availability needs, as possibly required by DoD COIs, on a device built for consumer acceptable levels of availability. This would include analyzing the availability of mobile applications with high availability needs when a security event occurs (degraded operations mode). This would also include protection against possible DoS attacks on mobile devices by utilizing security event responses (wiping the device or lockout). (AU-5) (SC-6) [33]
- Modifying the Identification and Authentication (I&A) on mobile devices.

        - This could possibly be performed by utilizing a combination wireless tokens and sensor information (behavioral and biometric) for continuous authentication. (IA-2) [33]
        - mobile devices authenticating to each other and their sensors. (IA-3) [33]
        - Mobile device authentication to the user. (IA-2) [33]
- Isolating, Sanitizing, or Downgrading information on single personality, or in the personality in its entirety. (MP-6)(SI-4) [33]
- Non-persistent personalities for highly sensitive information (SI-14) [33]

These mobile security policy topics are addressed in more detail in the future research section of the paper.

III. MOBILE DEVICE INFORMATION FLOW AND POLICY IMPLICATIONS

A. SECURITY OBJECTIVES AND STATEMENT

A mobile device that is used for processing unclassified information for the DoD must implement a security policy for a given functionality. This security policy should cover where information flow is allowed and disallowed and where information must be guaranteed to flow. This information flow is derived from objectives an organization is trying to achieve. These objectives are obtained from the functional requirements and Organizational Security Policies (OSPs). The organizational policies originate from Executive, Federal, and Department of Defense (DoD) Information Assurance (IA) policies. These policies are then turned into security controls that govern the information flow of the system.

As we stated above, we will begin with our functional requirements. These functional requirements will need to support use cases such as integrated personal calendars, real-time intelligence, automated supply, and remote health tracking. These use cases can be summarize into a functional summary for the device. This functional summary would be “a single mobile device that can process digital and environmental information from all aspects of a user’s life, while presenting such information at the right place and time in a consolidated manner. “

Our proposed functionality summary would have to be accomplished, while still complying with the organizational security objectives we listed earlier in this document. Specifically we will focus on the organizational security objective derived from DoDI 5200.01 and Executive Order 13556, which states “Controlled Unclassified Information shall be identified and safeguarded.” [84]. We propose that such a mission statement and objective could be achieved through a device that has multiple personalities on a mobile device.

When we have a mobile device with multiple personalities that fulfills this mission statement, there are additional threats and complexities that arise in protecting DoD information. A large number of these complexities arise because multiple COIs may exist on a mobile device on a mobile device, with shared resource (e.g., storage, sensors, network interfaces), but the different COIs may have different security objectives and policies than those of the DoD. We have listed these security complexities and threats earlier in this document, but we can summarize them as follows:

- Non-DoD COI, with a different security policy, compromising the Confidentiality, Integrity, or Availability (CIA) of a DoD personality
- User activity in non-DoD COI's personality generating CUI or sensitive information that requires protection
- Non-DoD COI allowing the mobile device to perform DoD restricted functionality due to the time or environment
- A command issued to a mobile device generates an activity that compromises CIA of DoD information due to context and personality
- The physical loss or tampering of the mobile device
- Mobile device not properly enforcing the COIs policies
- Conflicting COIs policies
- Manufacture or ISP compromising the CIA of a DoD personality

These threats should be addressed by our selection of security controls that drives the security policy and information flow on such a mobile device.

In summary, our security policy objective is to protect DoD information on a mobile device.

B. CONCEPTS FOR IMPLMENTING MOBILE DEVICE SECURITY

We have now identified the security objective to protect CUI from a DoD perspective. We did this while also identifying our functional requirement of a single mobile device that can process digital and environmental information from all aspects of a user's life, while presenting such information at the right place and time in a consolidated manner. We now link these requirements and objectives to an information flow and discuss how this information flow could be implemented with our previously discussed controls.

Considering our first use case of an "integrated personal calendar" as an example, we suppose there are multiple independent security domains on the mobile device. We continue to refer to these domains as personalities. Idealistically each one of these domains would be isolated from the others to guard against our previously developed threat list. Except that we wish to provide the user a common interface. Figure 11 illustrates this concept.

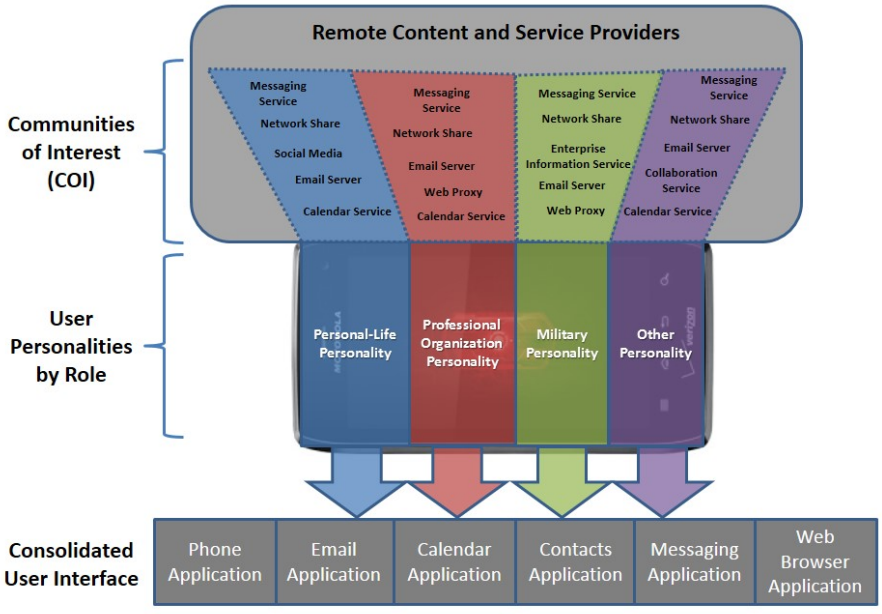

Figure 11. Multiple Personality Mobile Devices

In **Error! Reference source not found.**, we have three COIs with defined information owners that provide remote content and services. The information owners in the above example are the device holder (e.g., personal life), employer (e.g., professional organization), and military. Each establishes or provides allowable services within that personality. These COIs then map to a personality on the mobile device, for which they have ownership. The mapping between COIs and personalities is not necessarily one-to-one. For example, the ISP or manufacture may be a COI with no direct personality presented to the user. Since there will be multiple COIs with their own security policies on the devices, we would want to ensure integrity and confidentiality of the COI owned information. This could be accomplished while making the information available by presenting it in a way that is beneficial to the user, through a unified interface. Consequently, we have the need for a referee for the personalities: a universally trusted process to act as the reference monitor [77] to manage the information flow.

The question then becomes what COI would drive the access control policy enforced by the reference monitor. From a DoD protection of CUI perspective, the DoD would consider their personality as the top hierarchy and all others as equal subordinates. Whereas, from the perspective of any other COI, they would consider their personality at the top of the hierarchy. As such, we find that the hierarchy depends on the point of view of each COI. Additionally, our use cases do not assume a defined number of personalities. There can be any number of personalities added to the mobile device as needed by the owner.

We recognize there are many approaches to implementing a mobile device information flow to protect DoD CUI. One can have a 100 percent DoD device implementing NIST controls, a “centralize information flow enforcement” where DoD is defining the enforcement based on the NIST controls, or a de-centralized approach where each COI defines the information flow for their respective personalities. Previously we addressed security controls in reference

to mobile devices. Considering these controls, security objectives, our use cases and threats we find the following list useful in guiding the development of the desired information flow:

- AC-4, Information Flow Enforcement [33]: This control guides the application of mechanisms such as domains, isolation, and data labeling.
- AC-16, Security Attributes [33]: This control ensures information is attributed to a particular domain or security level. In our terminology this control would label the information for a particular personality.
- AC-19, Access Control for Mobile Devices [33]: Organizations will have usage restrictions the mobile device would have to support in an automated fashion if possible. An example would be turning off capabilities such as Wi-Fi or sensors such as the camera.
- AC-25, Reference Monitor [33]: Any device must have a trusted layer which provides basic security assertions required to meet the COI security enforcement.
- SC-16, Transmission of Security Attributes [33]: This control ensures information is attributed to a particular domain or security level when transmitted to and from the COI services.
- SC-8, Transmission Integrity and Confidentiality [33]: This control ensures the mobile device provides the mechanisms to ensure that confidentiality and integrity is maintained between the personality and COI.
- AC-XX Events Driven Access Control: This control ensures the mobile devices provides mechanisms to dynamically alter the information flow based on environmental context awareness.

- SC-XY Multiple Independent Security Domains: This control provides guidance for mechanisms supporting independent multi-personality information flow.

These controls will be considered in the following section along with the proposed implementations of mobile device information flow enforcement.

C. APPROACHES TO MOBILE DEVICE INFORMATION FLOW ENFORCEMENT

Now that we have defined the organizational objectives and security controls that govern our information flow, we can begin to define the information flow for the mobile device. For this to take place there must be management of the information flow to determine the hierarchy and mediation of conflicts among security policies. We demonstrate centralized and decentralized with trusted user conflict resolution as two possible approaches of enforcing this information flow, along with the conflicts and concerns that occur with multiple security policies on one mobile device.

In centralized enforcement of the information flow on a mobile device, a single organization explicitly coordinates or determines the device policy. For devices processing CUI, it would likely be the DoD defining the enforcement based on the NIST controls. In decentralized management of information flow on a mobile device, each organization on the mobile device defines their own policy. The device must then be capable of implementing each policy and their combination resultant policy, while allowing the user to resolve conflicts. In both approaches, one applicable implementation mechanism is a “reference monitor” [77] to fulfill AC-25 [33] control requirement listed above. We will use these two approaches to illustrate the questions, conflicts, and concerns with managing an information flow using multiple security policies on one mobile device.

In decentralized management of information flow on a mobile device, each organization on the mobile device defines its policy. The device must then be

capable of implementing each of these policies and their combination resultant policy, allowing the user to resolve conflicts. In both approaches, one implementation mechanism to apply is a “reference monitor” [77] to fulfill AC-25 control requirement listed above. We will use these two approaches to illustrate the questions, conflicts, and concerns with managing an information flow using multiple security policies on one mobile device.

1. Decentralized with Trusted User Conflict Resolution

Decentralized information flow enforcement allows each COI to define their security policy and resultant information flow, while allowing the user to perform conflict resolution between the COIs on the mobile device. To enable this, we have divided the standard notional mobile device architecture [74] (depicted below in Figure 13) into three layers of information flow enforcement. These layers are device, personality, and resulting set. The device layer is composed of the hardware, firmware, and OS contexts. This layer performs as the reference monitor and enforces mandatory access control between the domains, or personalities, based on labels for each CUI. The second layer is the personality. It consists of the application and information contexts in the diagram below, except that each layer would be reproduced for every personality on the mobile device. The personality layer provides the COI defined security policy and information flow. It is important to note that each personality provides its own distinct access control list. This list is bounded by the available system resources. The third layer is the resulting set of all the personalities and the device’s information flow enforcement layer. The resulting information flow is bounded by the device level information flow enforcement.

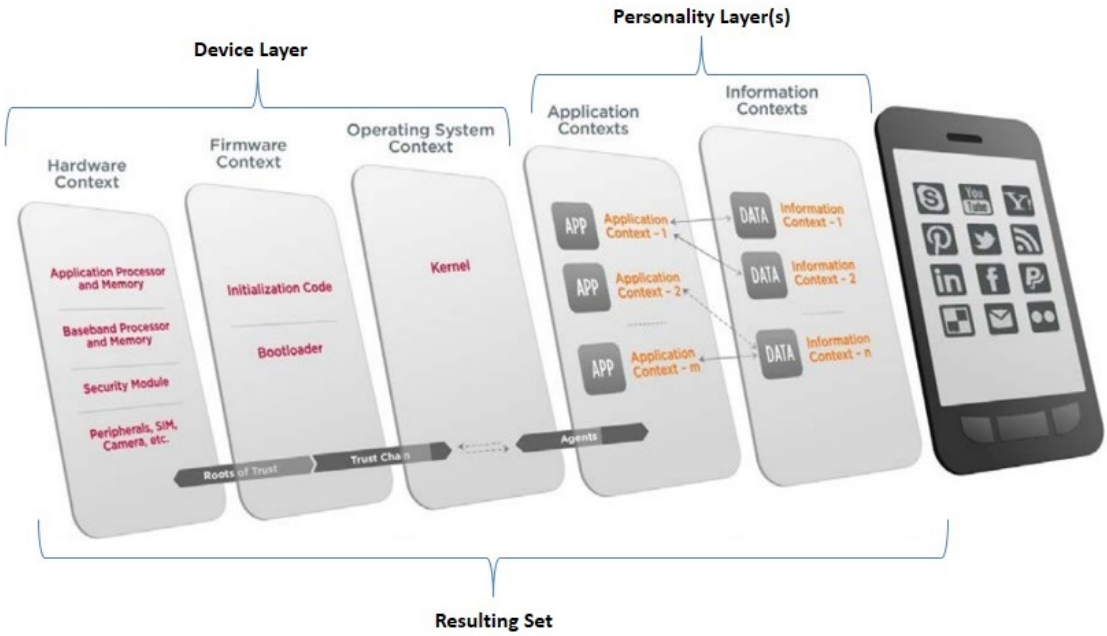

Figure 12. Standard Notional Mobile Device Architecture After [74]

In decentralized management with trusted user conflict resolution, each COI brings at least one personality layer, which resides on the device layer. The combination of these layers provides the system policy. This combination may cause conflicts at personality integration or runtime. With this information flow management type, the user is verified and trusted by each personality on the device to resolve these conflicts at both installation and runtime. This has some similarities to Android's application permission model [85], and may have comparable benefits and drawbacks [86] when it comes to conflict resolution. The identification of these conflicts and the potential concerns is the intent of this section.

a. Personality Information Flow Enforcement

One of the first controls we would want to asses in this methodology is AC-4 [33]. Specifically, ensuring that the flow of information generated by the user or environment only reaches the correct personality. One dynamic approach of assuring this flow would be blocking information flow to all personalities but one based on the environment or user perceived threats. An

example of this would include the AC-19 supplemental control of prohibiting the use of internal or external modems or wireless interfaces within the unclassified mobile device. This would take place at the device layer of information flow enforcement, where all other personalities are locked out through either user initiation or by an external environmental event. In a user-initiated lock out, the user simply activates one personality. Alternatively, said another way, the user can deactivate all but one personality. A lock out could be initiated when a certain context event occurs. For instance, imagine there is a lab where the COI security policy objective only allows the single use of the "lab personality" while employees are located in the lab. One could imagine the mobile device, communicating with some proximity sensor, where the device is used as a token to grant access to the user. In this scenario, the mobile device would recognize this event, triggering the mobile device to launch the correct personality and block the operations of any other personalities on the device. When the employee scans out of the lab, the device then clears the lock out and returns all other personalities to operation. The immediate question is what to do with conflicts?

First, we assess the environment. What do the personalities on the device represent and are they comparable? In the case where the personalities represent different comparable levels of security such as in the national security description of Confidential, Secret, and Top Secret, the requirement goes from not only being able to lock out other personalities but also being able to restrict a personality to operating only during certain events. Take our lab scenario, what if the lab where classified? This would assume the lab personality is classified, therefore one would not only want to lock out the other non-classified personalities, one would also want to ensure the lab personality locks itself out when the device is not in the lab. This could present a problem because what happens if the context is not received for exit from the lab? Would the policy/mechanisms allow the user to clear the personality lock? If that were allowed, the required mandatory access control could be defeated.

Applying the mandatory personality lockout scenario to non-comparable environment we find there still exists the possibility for conflict. In this environment, the multiple personalities are separate domains, but they are non-comparable from a security level consideration.

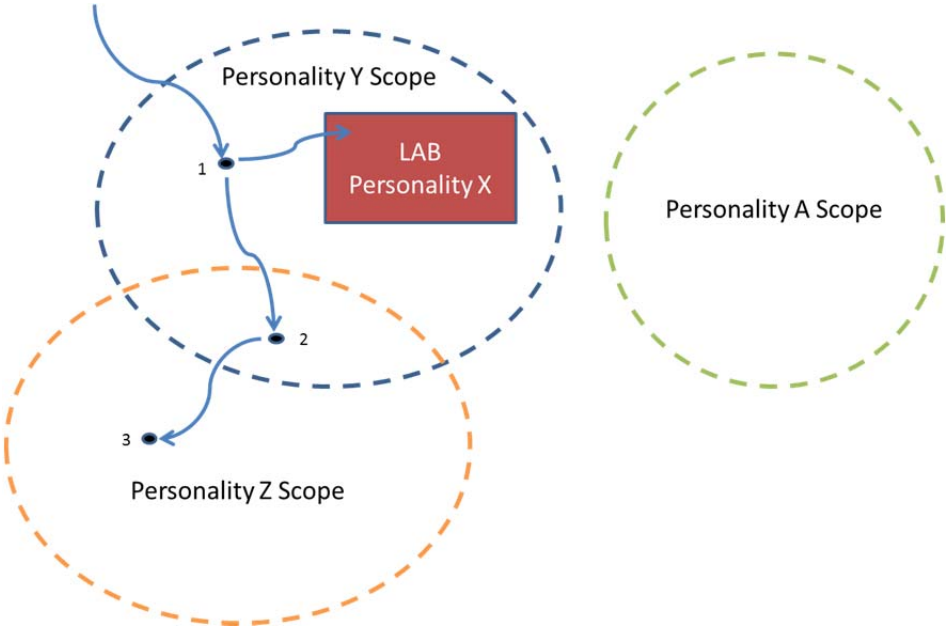

Figure 13. Personality Conflict Demonstration

Using Figure 13, we discuss a few scenarios which can lead to conflicts. It may be useful to think of the circles as representing physical spaces and the trigger event being location. However, the circles could represent any scope of a trigger event, the concept we are exploring is when there are overlaps and how those conflicts should be resolved.

As the user causes the trigger event for personality Y, the mobile device may lockout all other personalities. This is the easiest case since the user is only “in” the one scope. However, if the user chooses to enter the lab, the scope of personality X, how should the mobile device handle the conflict since X exists entirely within Y? In this scenario, we could imagine that the lab physical access control process is the context for changing the information flow. Maybe the lab only allows the user to enter once the device is set to the X personality

with the information flow for all other personalities blocked. Otherwise, the user would have to leave the mobile device outside the lab. (It is also worth noting how the environment could have indirect control over the overall security policy. Consider the case where a third party Lab requires visitors to leave their mobile device outside the lab. This sacrifices our availability for their confidentiality. In this case the environment adds another layer of complexity to the actual implementation of our COI security polices.)

What if the user moves to the area of point 2? The user is currently using the Y personality information flow but moves into a territory where the Z personality information flow overlaps. Should the user get a notification? In this scenario, we propose the user would have to be the mediator.

Going back to the previous example, if the lab was not a physical place but just a scope that existed entirely inside the Y scope, the user would have to mediate the conflict, otherwise the X personality would be entirely locked out from use and we could potentially see a denial of service vulnerability in our construct. In fact, one possible construct of this information flow is that the user can always mediate the personality conflicts and set a particular personality to lock out all others, and release lockouts.

We note that this is a discretionary access control approach of the personalities, the user controls the access, and therefore this mechanism does not work for scenarios where the personalities require some form of MAC, outside of the user's discretion.

Alternately, conflict resolution could be determined at personality installation. During this time, the information flow of the personalities could be reviewed against the new personality and conflicts could be determined. In this way, the installer (user/administrator) could be asked to resolve the conflict by selecting a personality to take precedent or we could simply choose to lock out both personalities.

In the case where the user can decide the precedence, the opportunity exists for the user to violate a COIs information flow intention. For example, imagine the Lab X personality is installed and then the user installs the area Y personality. When the conflict is identified the user then selects area Y to take precedence. Therefore, when the user enters the Lab with their mobile phone it will remain in the Y personality and violate the X personality information flow. From a DoD perspective, if X represented a DoD personality this would violate our security policy objective. Essentially, this form of conflict resolution maintains a MAC access control but trades confidentiality for availability of the user's preferred personality.

In the case where conflicts are resolved by disabling both personalities during conflict we are essentially saying the device is unusable during all personality conflicts. In these cases, the intent is to protect the confidentiality of a given personality, this means all other personalities must cease to be able to use the mobile device in the given context. Therefore, when locking out all the personalities that believe they have a need for confidentiality we essentially lock out the entire device. In this case, we are again keeping the MAC access control but now trading availability for confidentiality.

b. Sensor Information Flow

Since the use of wearable computing devices and sensors with mobile devices is increasing, attention will have to be place on this information flow for all forms of management (e.g., centralized or decentralized). These sensors will be a shared resource for information about the outside world to the different domains, or personalities, available on the mobile device. The information owners associated with each of these personalities (or COIs) will determine the information protection needs for their data. As such, we believe specific attention will need to be place on controlling the flow of information between the sensors and the different personalities on the device. In order to accomplish this, we are defining a potential information flow to provide each

domain the confidentiality, integrity, and availability needs for the information provided by these sensors. These “sensor” flows will change depending on the environment of the mobile device.

The context of the user’s situation may determine the sensitivity of the information obtained from a sensor. That sensor information may be sensitive for one COI (e.g., military), but get recorded for another COI (e.g., personal). For example, when an application is retrieving sensitive (e.g., CUI) sensor information in a military domain, it may be the case that the personal domain should not be allowed to pull the same sensor information concurrently or even a second later. Additionally, sensors could exist on the device that should only provide information to one personality.

One confidentiality example could be the Scanadu SCOUT [25], which provides health information that the user may only want provided to the “personal” personality. One availability example could be an additional more accurate military GPS sensor that provides constant uninterrupted GPS to the military COI only. These are some of the concerns that we are looking to solve with the information flow described in this section.

The information flow we propose does not require coordination among COIs on a mobile device, or a coordinated security policy. Each COI would provide its own sensor policy upon deployment of a personality. That policy could consist of 4 fields, which are defined as follows:

1) Sensor—A unique identifier for a sensor’s service, below the personality level, for which the policy is being created. Examples of these sensors could include GPS, Camera, fitbit [9], Scanadu SCOUT [25], or Square [15]. If two GPSs are attached to the device, the sensor is still classified as a GPS sensor.

2) Allowed—A field that identifies if that sensor is allowed to be utilized by the COI.

3) Context Trigger—A context trigger is a field that contains environmental events, called “context events,” that would restrict the use of a specific sensor by all other COIs until the environmental event passes (e.g., entering or leaving a circular area centered on a GPS-identified location). We call this restriction on the use of sensors an “Information Flow Block” (IFB). This IFB helps protect the confidentiality of the sensor information in a given contextual event. Examples could include location, time, motion, variance of sensor information, or ownership (see below).

4) Owned—A special permanent context trigger that grants the COI full ownership of a sensor with no other COIs having the ability to access its information. This field is here to provide greater availability or confidentiality for a sensor’s information to a particular COI.

An intersection of the policies of each COI on the mobile device is then used to enforce the information flow based on “security policy load,” “context triggers,” and “sensor access requests.”

Even though no coordinated security policy exists among the COIs, there may be times when the security policy will need to be mediated among personalities. One reason for such a mediation could be to allow or disallow a personality from block the information flow on a sensor to all other personalities on the device through broadly defined context triggers (e.g., time is infinity, or GPS location is the entire earth). This mediation would likely need to take place prior to the triggering context event occurring, otherwise there are risks of compromising a personality’s confidentiality, integrity or availability.

That is way we chose to have “conflicts” and “threshold” checks upon personality load and security policy changes (e.g., changing context triggers or ownership). Conflicts are when two personalities have the same, or overlapping context triggers. An example would be two COIs requesting exclusive access to GPS information in overlapping geographical areas. Thresholds would have to be predetermined or user defined thresholds

established on which personality owns or controls the information flow blocking of a sensor. An example of a threshold could be a context trigger with a 500-mile or larger radius around a GPS coordinate provided by a COI. One approach to resolve these “conflicts” and “thresholds” might be to have the user make a determination on if such “conflicts” and “thresholds” are acceptable on the mobile device. If such an approach was used, a personality could be loaded or security policy changed upon the following criteria being met:

- Upon personality load or change in security policy, the user is notified of conflicts among personalities. The user is also notified that any context events for which there are conflicts, the corresponding sensor will be disabled for all personalities. The user is then provided the option of continuing to load the personality, or completely back out of the load. If back out is chosen, the personality is not loaded and security policy remains the same.
- The user is notified of any context event thresholds that go beyond the defaults on the mobile device or previously user defined. These thresholds could include ownership, time equaling infinity, or an extremely large GPS area. The user is then provided the option of continuing to load the personality, or completely back out of the load. If back out is chosen, the personality is not loaded and security policy remains the same.

It is important to note that throughout the criteria above, the user will never be able to change a COI’s provided security policy. They are only able to agree or disagree with the effects that loading a personality will have on their device, thereby agreeing to load the personality or not.

The next piece of establishing the information flow is an “Information Flow Block” (IFB), which is initiated when a context-based event occurs for a specific personality, as annotated in their sensor policy. Examples of these events could include a GPS location, time, or proximity of a wearable

computer (i.e., uniform or access card). The IFB of the sensor is then released upon leaving the contextual event. The information flow for a sensor information flow bock request is as follows:

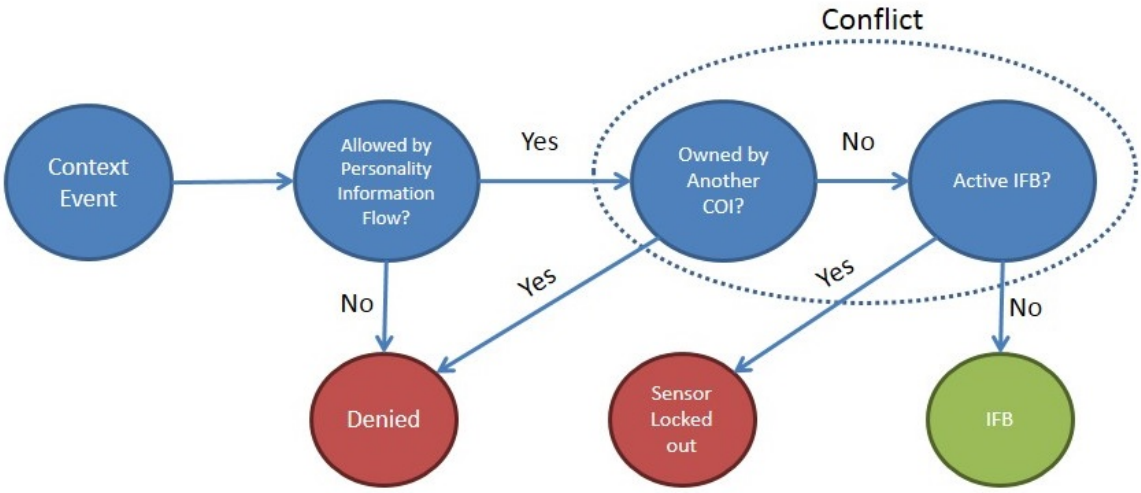

Figure 14. Mobile Device Information Flow—Information Flow Block Request

Using the information flow in Figure 15, one approach for a personality to provide an information flow block of a sensor would be if the following three criteria were met:

1) The personality is allowed access, based on the COIs policy, to the requested sensor that initiated the context event.

2) The requested sensor that initiated the context event is not owned by another COI. This is a potential conflict, which is discussed below.

3) The information flow to the requested sensor that initiated the context event is already blocked by another COI. If such a block is present, than there is a conflict which is discussed below.

Of the criteria above, two and three have the possibility of a conflict occurring with other personalities on the device. The first conflict exists if another

COI owns the sensor for which a context block is being requested. Since a COI's sensor ownership overrides any other CIOs access to a sensor, this conflict is immediately resolved by automatically denying the requested information flow block. The second conflict occurs when two or more COIs have an information flow block for the same contextual event. An example would be two COIs requesting exclusive access to GPS information in overlapping geographical areas. This conflict is not automatically resolvable since no one COI has precedence over another, so the sensor is locked to all personalities on the device until one of the contextual events passes. Continuing, a contextual event could be leaving the geographical area that has the overlapping contextual trigger.

A "sensor access request occurs" when a personality requests access to a specific sensor. This information flow for this request is as follows:

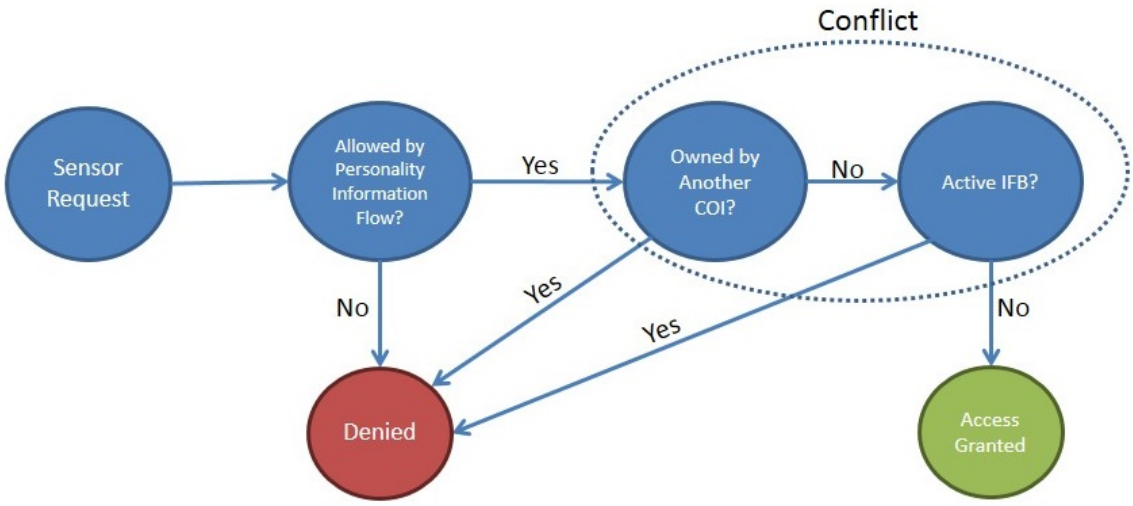

Figure 15. Mobile Device Information Flow—Sensor Request

Using the information flow diagram above, a personality receives sensor access if the following three criteria are met:

1) The personality is allowed access to the requested sensor based on the COIs policy.

2) The requested sensor that initiated the context event is not owned by another COI. This is a potential conflict, which is discussed below.

3) The requested sensor is not blocked by another COI. If such a block is present, than there is a conflict which is discussed below.

Of the criteria above, two and three have the possibility of a conflict occurring among other personalities on the device. Both of these conflicts are encountered when another personality has temporary or permanent exclusive access to the sensor, resulting in the requested access being denied.

Now that we have defined the information flow for sensors using personalities, we believe that it would be useful to provide an example set of COI sensor policies. These example policies would then be used to analyze their impacts on the threats we described above. These examples involve a user with both a military and personal personality. Our proposed sensor policies for these two personalities are as follows.

SENSOR	ALLOWED	CONTEXT TRIGGER
Camera	Yes	1) 30 mile radius around deployed location
GPS	Yes	2) 30 mile radius around deployed location 3) Uniform Sensor within 6 feet
Scandu SCOUT [25]	Yes	No

Table 3. Military COI Sensor Policy (provided at personality load)

SENSOR	ALLOWED	CONTEXT TRIGGER
Camera	Yes	No
GPS	Yes	No
Scandu SCOUT [25]	Yes	Owned

Table 4. Personal COI Sensor Policy (provided at personality load)

COI	SENSOR	ALLOWED	IFB ACTIVE	OWNED
Military	Camera	Yes	Yes	No
Military	GPS	Yes	Yes	No
Military	Fitbit [9]	Yes	No	No
Personal	Camera	Yes	No	No
Personal	GPS	Yes	No	No
Personal	Scandu SCOUT [25]	Yes	Yes	Yes

Table 5. Mobile Device Sensor Policy

The three scenarios, based on sensors, that we will be assessing against this policy are “Silence is Information,” “Walk in the Woods,” and a part of “User Privacy,” discussed in section I.D3. We will be assessing these threats

present in these scenarios by following a military user through activities that show these potential threats and how the policy might address them.

Silence is Information: While at home, a military user finishes posting his last picture of wooded scenery prior to leaving for deployment on a sensitive mission. Before leaving the house, he puts on his uniform that contains embedded military sensors that can communicate to his mobile device. These sensors trigger a change in context for the mobile device, in accordance to context trigger 3 of the Military COI Sensor Policy. This restricts his GPS location to the military personality, blocking the information flow to all other personalities. Since his friend tracking service in his personal personality was constantly pulling GPS location information, it only locates him with his last known location. In this case, that location would be his home (not miles from the deployed location). He then jumps in his car, turns on his military GPS navigation software, and heads off to fly out.

A Walk in the Woods: A short while later, this military user enters a cargo aircraft for transportation to the deployed location. After a long flight he comes within 30 miles of his destination. This change of contexts activates context trigger 1 of the Military COI Sensor Policy. This context trigger restricts his camera to his military personality only. As he arrives and steps out of his aircraft, the military user notices some curious wooded scenery. He takes out his mobile device and attempts to take a picture to post to his favorite social network. Since the camera is now restricted to his military personality, that photo is not possible. As he starts to put his camera away, he notices something interesting regarding local insurgents in that same wooded region. He pulls his camera back out and takes a picture, which he immediately shares using an intelligence application.

User Privacy: After a short walk to his barracks, he once again pulls out his mobile device. In doing so, he accidently attempts to access his health information from his Scandu SCOUT [25] in his military personality. Since his mobile device sensor policy states that the Scandu SCOUT [25] is owned by

his personal COI, the access is denied. Thus preventing the military personality from accidently accessing his private health information.

c. Personality and Unified User Experience Information Flow

We believe that there should be a unified user experience that presents the information from different personalities in a consistent consolidated fashion for at least a defined subset of the functionalities provided by each personality. But as stated earlier, personalities are implemented through domains on the device with the information on the device controlled by the information's owners, or COIs. Each of these COIs bring a security policy to implement on the device, with no explicit information flow among the personalities owned by different COIs. Nevertheless, we believe that a unified experience should still exist. We propose that this might be accomplished through trusted applications. Examples of such applications could include notifications, phone application, email application, calendar application, contact application, and messaging application.

Trusted applications are high assurance applications trusted to aggregate or control the flow of information from separate COIs for presentation to the primary user of the mobile device. The information presented by a trusted application would be in compliance with predefined fields, or a summary. In other words, it would not present the entire contents of that COI's application, just a summary, to protect the confidentiality of this information. Each COI would be able to define what information could be presented in this summary, or if any summary should be available at all. For example, the email application may have the following predefined fields available: sender's email address, subject line, and time. When selected the trusted application would launch the corresponding application in the personality of the information selected. For example, if a military COIs email was selected the email application of the military personality would be launched. The initial information flow might be as follows:

- Each COI would select which trusted applications it would like to interface with in the trusted application portion of its policy.
- Each COI would label the information that it would like to be presented to the trusted application based on the label documented in the trusted application portion of its policy.

The information flow among the trusted applications and personalities would be as follows:

- The trusted application is allowed to read the corresponding application's labeled summary information within other personalities in accordance to the defined COI policy. For example, the trusted email application can read the email addresses, subject line, and time from the personal and military personalities on the device.
- The trusted application is allowed to execute the corresponding application within a personality. For example, when a military email is selected in the trusted application, the military personality is launched with its email application.

All other information flows among the personalities and trusted application are prohibited. A diagram of this information flow is listed below, where TP_{alpha} is the trusted application with which the user interfaces.

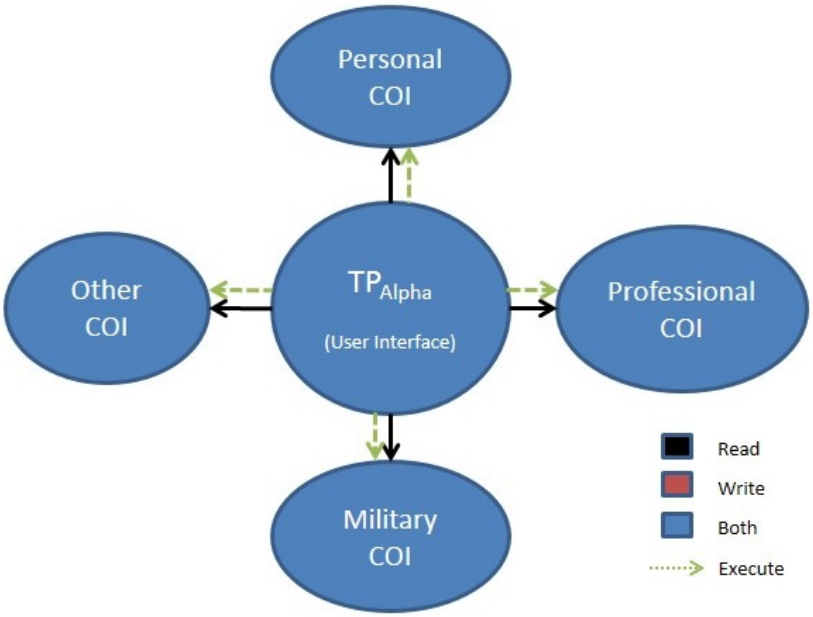

Figure 16. Trusted Application

d. Analysis

Now that we have described our approach to the information flow enforcement on mobile devices, we can compare it against the controls we previous noted as being particularly useful in guiding the implementation. We analyze, for each control, how our approach satisfies the intent:

- SC-XY Multiple Independent Security Domains: In our approach, we define separate personalities that maintain security levels isolated from each other personality. These personalities also decide what information is available, read only, to the provided trusted applications, for example the consolidated calendar user case.
- AC-XX Events Driven Access Control: In our approach, the information flow is dynamically altered based on environmental contexts that are defined by the information flows of each personality/COI.

- AC-4, Information Flow Enforcement [33]: The mobile device layer provides the mechanism for this control. However, as identified in our scenario, this mechanism is diminished by the possibility of conflict between each personality.
- AC-16, Security Attributes [33]: This control supports the information flow by labeling information according to the personality. Our approach currently assumes container separation where the container is the personality and there is context aware control of the sensors. Our approach does not include the use of security labels. However, an alternative approach would be to use security labels at either the personality level or the file level. It may also be useful to implement labeling within the personality in order to distinguish between levels of sensitivity of information. For instance, the DoD personality may require labeling for PII or other types of CUI.
- AC-19, Access Control for Mobile Devices [33]: Our approach implements personality information flow block outs at the functional and sensor levels to implement personality/COI policies. Container-based encryption could be used to isolate personalities.
- AC-25, Reference Monitor [33]: The mobile device layer would provide the reference monitor functionality to enforce the information flow. The flow of information from sensors and to and from the trusted applications relies on the reference monitor which implements the “events driven access control.”

- SC-16, Transmission of Security Attributes [33]: This control supports the information flow by maintaining the label of each piece of information during personality or COI the transmissions. Our approach currently assumes container separation. However, an alternative approach would be to use security labels.
- SC-8, Transmission Integrity and Confidentiality [33]: Communications between the Personality and COI services are implemented with encrypted communications provided by the applications within the personality layer as needed based on the “events driven security context.”

We find that there are potential conflicts that arise when multiple COIs reside on a device without a coordinated security policy, especially where the personalities’ security levels are non-comparable. These conflicts occur when the security policies among two or more COIs overlap. Since these COIs’ security policies are non-comparable, no one policy takes precedence over another. This has the potential of leading to a security policy violation for one or more of the COIs which have the overlap. We identified a possible way to approach these conflicts through user mediation at either time of conflict or personality install.

The first option allows the user to select the personality that should take precedence, leaving the user to decide which personality represents the user’s current actions on the mobile device. But in doing so, this options creates a DAC policy and allows the user to potentially violate a COIs security policy. The second option allows the user/administrator(s) to address the conflicts ahead of time, at personality install, and therefore maintain a MAC policy and increase the confidentiality level provided. But in this option, the availability of a personality could be sacrificed along with the following additional potential drawbacks of:

- Conflicts being presented in too broad or too detailed of a fashion, leaving the user not able to truly understand the conflicts
- The user may “just click through” or past the conflict to complete the personality installation ignoring or not aware of the conflicts that could arise
- The user may not have all the requisite information to make such an appropriate decision

2. Centralized

In this demonstration, a centralized information flow enforcement allows one COI to define the security policy and resultant information flow for the mobile device. This could be done through a COI mandating their own specific information flow, coordinating a security policy with other COIs, or perform conflict resolution among the COIs on the mobile device. In this demonstration, we selected the DoD to be this centralized managing organization.

a. DoD Centralized Management

These approaches are very similar to our decentralized approach except that the DoD either owns the device, coordinates a security policy, or performs conflict resolution. Each of these approaches has its own benefits and negatives for the user and DoD. When the DoD owns the device, they provide the device to the user with only one or two personalities, which could be “DoD-only” or “DoD and personal.” The DoD only device already exists and would not meet a majority of our use cases, so that would not be an option. The DoD and personal personalities would meet a portion of our use cases, except any other COIs (e.g., professional organizations or second jobs) would not be able to provide their own personality. In this approach, the DoD resolve, through the use of AC-19 MOBILE DEVICE ACCESS CONTROL, all conflicts by giving preference to the DoD personality, thereby protecting CUI at the cost of availability to personal personality.

In the coordinated security policy approach, the DoD would chair a coordination meeting with the other COIs to create a security policy that is comparable with a hierarchy or resolve all policy conflicts at that time. This option would meet all of our use cases, but is not feasible since the DoD is not likely to sit at the table with every possible COI. Hence this approach not a likely or feasible option.

In our last approach the DoD's policy is at the top of the hierarchy, above all other COIs, for conflict resolution. The DoD resolves, through the use of AC-19 MOBILE DEVICE ACCESS CONTROL, all conflicts by giving preference to the DoD personality, thereby protecting CUI at the cost of availability to all other personalities on the mobile device. In this approach someone would still have to resolve the security conflicts among all the non-DoD personalities on the device.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CONCLUSION

A. SUMMARY

As we conclude this thesis, our research shows there are many security concerns regarding multiple personality mobile devices given the current technologies and policies. We have illustrated how all these issues arise in examples but research will have to be conducted to determine how best to resolve them. We have provided some examples of this research below. Where possible, we have also provided potential references to help guide this research, and demonstrate the work that has already taken place on these topics. Finally, in our conclusion we summarize our approach to mobile device security, analysis and results.

B. TOPICS FOR FUTURE RESEARCH

1. Declassifying, Sanitization, and Downgrading

There may be some issues with implementing the process of isolating, sanitizing, or downgrading a single piece of information on a personality, or the personality in its entirety. When performing these actions on a personality, it would be ideal to not negatively affect the other personalities on the device. For example, if there is an incident (security violation) that occurs on one personality, it would be ideal to have that personality completely isolated from the others on the device, while leaving the non-affected personalities available. If the threat is deemed to be large enough, it would also be ideal to have the capability to remotely wipe individual files or entire personalities without destroying the non-affected personalities. There are similar concerns with sanitizing and downgrading information.

In regards to sanitizing, currently documents like the “NSA/ Central Security Service (CSS) storage device declassification manual,” require sanitizing solid state devices by “smelting in a licensed furnace at 1,600 degrees

Celsius or higher or disintegrate into particles that are nominally 2 millimeter edge length in size using an NSA/CSS evaluated disintegrator" [87]. For flash memory, sanitizing is performed on "Electrically Erasable Programmable Read-Only Memory (EEPROM) by overwriting all locations with a known unclassified pattern" [87]. While in the NIST SP 800–88, they recommend that PDAs have all information manually deleted, along with performing a manufactures hard rest to the factory state. [88] All four of which, would destroy all other personalities on the devices since it destroys the data across the entire drive. It would be interesting to see if there is a sanitization process that would leave the other personalities intact, some sources that may help with this research include: [89], [90], [91], [92], and [93].

Along the same line of thought, with the introduction of sensors, the classification of data may be dynamic, for example depend on the context. The classification of sensor data may change as we showed section I.D.3 "silence is information" example. The ability to dynamically manage the classification of this information among personalities, along with the ability to correct errors that occur, could be a topic for future research.

2. Non-Persistent and Thin Personalities

In regards to cyber-attacks against highly sensitive or widely exposed personalities, it may be useful to mitigate against advanced persistent threats by significantly reducing the targeting capability of adversaries (i.e., window of opportunity and available attack surface). This could be done by making the targets non-persistent through "domain virtualization" with automatic deletion/restoration on mobile devices.

There may be times that the data is so sensitive that you would not want the applications or data to leave the corporate network or even confined the data to a specified physical area. This problem may potentially be resolved or mitigated by having a "thin" personality that is only available on the corporate network within the corporate physical building. When the mobile device is not on

the corporate network and within the physical confined area, the personality would no longer be present. The papers that could help assist with this future research are: [94] and [95].

3. Information Flow among Personalities, Sensors, Network Infrastructures, and Enclave

The use of wearable computing devices and sensors with mobile devices is increasing. A large topic for future research would be the information flow among personalities, sensors, and wearable computing devices. This topic is multifaceted and involves integrity, confidentiality, and priority of access.

For confidentiality, as described in section I.D.3 with the example “Silence is Information,” the environment or context of the user and mobile device may determine the sensitivity of the information obtained from sensors. Based on this context, sensor information may be sensitive for one COI (e.g., military), but another COI may consider the same information publicly releasable (e.g., personal). The question then becomes: when an application is retrieving sensitive (e.g., CUI) sensor information in a personality, such as DoD, should a non-DoD personality be permitted to pull the same sensor information concurrently, or even a second later? This is not the only confidentiality issue. Wearable computing devices are also going to provide access to additional personally identifiable and health related information (described in section I.D.3). The management and release of such information, and more, may be controlled by laws, regulations, and privacy concerns that would need to be addressed (e.g., HIPPA and PII). Hence, the information flows of sensor data is an essential confidentiality concern. The easy solution would be to turn off these sensors and wearable computers, but a good future research topic would be to discover how to securely enable this technology in the appropriate personality and achieve the benefits it could provide.

The integrity of information provided may also be essential to these wearable computing and sensor devices. Vital decisions may be made based on

the information provided by these sensors, such as military locations for the DoD or health status for the person. We would want to ensure that the correct information is coming from the correct sensor. One way to accomplish this is by providing mutual authentication between the personality and wearable computing devices/sensors. This way there is assurance that the information provided by these sensors is actually coming from the correct source. It would also be an interesting research topic to determine the feasibility of assuring the information from these sensors is accurate, and not being falsified or modified.

Availability may also be essential for personalities and their wearable computing/sensor devices. Applications may require continuous uninterrupted access to a sensor. In order to ensure the confidentiality of information from these sensors, different COIs may also want to ensure that no two personalities have access to a sensor at the same time for a given situation. It is resolving this inherent conflict that would be a topic for future research.

4. Information Flow among Personalities, Network Interfaces, and COI Infrastructures

Mobile devices have expanded the possible ways of obtaining network connectivity. In fact, the methods of accessing various network infrastructures may increase and become even more complex (e.g., mesh networking). When you combine this with multiple personalities existing on a device with various security needs, the topic becomes more interesting and more complex. That is why the information flow controls between the personalities and the network interfaces and enclaves is an area of future research.

The first area that needs to be addressed is, communication using the mobile service carriers. Currently most mobile device's external boundaries are managed by mobile service carriers. These boundaries would need to be monitored. This may need to be addressed through a strong partnership with mobile service carriers. An interesting question is, who owns the results from

monitoring activities. Another approach could be VPNs back to the COI organizations network defense. In this case, there are several layers of monitoring that would have to be integrated.

The next area that needs to be addressed, and is a potential area of future research, is communications taking place over alternate interfaces and infrastructure. By alternate interfaces and infrastructure, we mean mechanisms other than the COI's or ISP's provided network infrastructure. The enablement of this functionality, dramatically increases the availability of both functional and security services. The most mobile unique example of such an infrastructure would be mesh networking [11]. Secure communications over these mesh networks, may be an important subject for future research. A potential approach would probably include unique device-to-device identification and authentication.

5. Privacy and User Rights

When a device is owned by multiple stakeholders, one of which is the user, privacy and user rights concerns come fore. These concerns arise from items such as auditing/monitoring, incident response, ownership of device/data, and configuration management. The level of privacy and user rights must be clear to the user to avoid invalid assumptions and misconceptions." They must also follow current rules and regulations, with possible modification to such rules and regulations being required. The rule and regulation modifications that might be required and how they could be securely implemented is a topic of future research.

6. Official Time Source among Personalities

Many services on mobile devices require an accurate and coordinated time source. Examples of such services include diverse areas such as Code Division Multiple Access (CDMA), auditing, and incident response. Different COIs may have different requirements for time synchronization across services deployed on the personalities. In addition the different COIs may insist on using different "time sources." These conflicting time synchronization requirements

could cause issues with incident response or even CDMA. An example would be if the policy requires the device to sync to a COI approved time source. Resolving or providing infrastructure to support these different times sources and applications needs to be studied further. Device-level use of UTC derived from GPS is possible (though able to be spoofed [96]) solution.

7. Mobile Carrier Access to Device

Current policies restrict the commercial mobile carriers access to mobile devices. Currently in the commercial sector, most patching/upgrading of the mobile devices is performed through privileged access provided by mobile service carriers. Resolving this apparent conflict between industry trends and DoD policy can be an area of future research. Possible solutions could include a strong partnership with mobile service carriers to uniquely identify and authenticate such access. This would also include a way to provide a level of authenticity and verification of accuracy for patches (i.e., DoD signed patches). Other solutions could include patching based on COI and personality, where the mobile carrier only provides patches to the COIs whose security policies allow it.

8. Coordinating Classifications/Confidentiality Levels

As mobile device personalities span different COIs, or organizations, the classification guidance for information stored on these devices may vary. This could cause security conflicts when such information is stored on the mobile device. An example of such a conflict could include, an organization considering one piece of information classified, while another organization considers it CUI. This could affect data flows, access controls, and overall classification of the device. Understanding, documenting and providing mechanisms for dealing with and/or resolving such conflicts should be addressed.

9. Utilizing Context Awareness for Security

Just as context awareness on mobile device can provide additional functionality not previously possible, the same is true for security services.

Context aware security applications could be utilized to enforce security policies in a way that simplifies security management for the user. Examples could include authentication, security logs, or enabling/disabling services (such as a camera in a SCIF). In fact, the commercial industry is already moving in this direction. Apple has filed a patent to enable different levels of authentication based on the phones location [97]. Finding and implementing these context aware services to increase the security posture of mobile devices while making life easier for the user is a topic of future research. One example of such a service for future research is detailed below:

Certain policies that made sense for the docked systems may not make sense for mobile devices that are context aware. We propose that pin and passcodes is one of those policies that may not apply to mobile devices. Forcing a pin or passcode prior to obtaining information from a mobile device might hinder functional use cases, or cause potentially dangerous security exceptions (as described in section I.D.3 with the example “alerting terrorists of U.S. friendly forces”). The user must still be authenticated to the device, but potentially using something other than a pin and token to provide something you have, know, and are. This is made possible because the device has the capability of context awareness along with additional detailed information about its user. A combination of something you have and something you are might be a preferable authentication mechanism.

The something you have, could be an authenticator (something you have) that is wearable, embeddable, or even able to be swallowed. This would then be combined with a biological or behavioral patter (something you are). This would allow users to stay authenticated to the device as long as the devices is “close” to the user. A passcode could then be used in a “break glass” situation where the biological or other authenticator is lost. Clearly more work needs to be done in this space to achieve the kind of assurances required for DoD and other uses. The integration of these capabilities with the different personalities also needs to be studied.

10. Security Services on Resource Limited Mobile Devices

There are a wide variety of security services that are currently deployed on our docked information systems. Some of these services include auditing, malicious code protection, IPS, and monitoring software. Planned and prioritizing deployment of these security services on resource limited mobile devices would most likely have to take place. This analysis could include selecting or developing scaled down versions of these services and the integration of these services with the various COI infrastructures.

11. High Availability Requirements

Mobile devices maybe the primary communication medium for their users to the outside world and may need a higher level of assurance for availability than their notebook or desktop counterpart. This can be demonstrated with functions that were previously performed over radio on the battlefield or emergency service, and are now taking place on mobile devices. This could become a potential conflict when the mobile devices are built for a consumer acceptable level of availability. Further research should take place to determine if there is a way to mitigate this risk, while still taking advantage of the cost and ubiquity of these devices.

Additionally applications that require high availability will require security protections such as DoS prevention, priority of communication services, and higher assurance of communication services/application. As we progress towards 4G/VOIP, DoS attacks and loss of availability may become more prevalent. Thus high availability may become more important. These availability requirements could be an area of future research, since they do not exist in current policy. Some example security approaches that could be included are redundancy in communication protocols and services; or a minimum set of communication applications available upon certain levels of device failure.

12. Choosing an Architecture for Mobile Devices with Personalities

Developing or choosing an architecture for multiple personality mobile devices could be an area of future research. This study could possible include analyzing other architectures and frameworks, such as type 1 or type 2 hypervisors. A part of this study could also include an evaluation of architectures and implementations currently on the market against the functional and security use cases for multiple personality mobile devices. Examples of potential architecture and implementation currently available for analysis include:

- Green Hills Software [98]
- OkLabs High Assurance Framework with LG [99] [100]
- Red bend vLogix [101]
- SELinux [102]
- VMWare Mobile Hypervisor with Samsung [103]

13. Choosing and Applying a Formal Security Model for Mobile Devices

Current security configuration documentation for mobile devices, such as the DISA SRGs, does not require the use of a formal security model. A possible topic for future research could be the selection and implementation of a formal model for mobile devices with multiple personalities. Such a model could be used to analyze the properties of such a system with a goal of providing assurances that the system will "behave as advertised."

C. CONCLUSION

Through the course of this paper we confront the issues surrounding mobile device security for today and into the future. Our main questions were:

- What is unique about mobile devices?
- What is the affect to security policy?

- Are the security controls affected?
- How is implementation affected?
- Is there a solution for implementation?

We address these questions systematically with the following results:

1. What is Unique about Mobile Devices

First, in Chapter I, we describe the problem by revealing what is unique about mobile devices. We first note how mobile devices are more “personal” than traditional computing devices in that they become much like a digital surrogate for the owner. Mobile devices are always on, always on you, and through their suite of sensors they are environmentally context aware. A more traditional computing device such as a laptop is typically used only for the purpose it was acquired. For instance, a work issued laptop is normally used in the work environment for work tasks. Whereas, at home one would have a personal laptop used for personal task and entertainment. Mobile devices, given their personal nature, tend to be used in both environments for both work and personal tasks. As such, there exists many different unique functional and security use cases for mobile devices.

2. Security Implications

In the process of examining the security implications of mobile device usage we identified the following use cases:

- User Calendar–Consolidated calendar view of all personalities
- Walk in the Woods–Location reporting for personal and DoD use
- Crashing a Video Party–Video conferencing for personal and DoD use
- Skyping from a SCIF–VOIP use for personal or unsecure communications and secure communications

Conversely, we noted the following cases that present specific security threats:

- CEO All Hands for Harry Potter–the invite for this party is sent to the work email contacts list versus only the personal list as intended
- Alerting Terrorist of U.S. Friendly Forces–Blue force tracking is running on a lost mobile device which then falls into the enemy hands
- Uncontrolled Unclassified Information–CUI is unintentionally saved to a personal cloud service
- False Notifications–a virus is downloaded on a less secure personality which masquerades as Blue Force Tracker application and successfully tricks the user
- Free Wi-Fi and the Battlefield–the device automatically attaches to a random Wi-Fi service which provides false information to the device
- Passwords, there is an App for that–a password management application stores passwords for all personalities on a less secure personality
- User Privacy–Private information is revealed to an employer through device monitoring. Based on this information the employer decides to terminate employment the employee.
- A Door to China–devices made in foreign nations may provide security holes or back-doors
- Silence is Information–a user whose “find my friends” application or other social networking sites go inactive could indicate they are deployed

After analyzing these specific use cases and threats against current DoD security policy objects we found them sufficient for addressing mobile security policy information flow. We then analyzed the lasted draft of NIST SP 800–53 revision 4 to determine the impact on the security control catalog. In this way we determined controls which were mobile interesting and required special consideration for mobile devices as well as those controls which were found to be mobile unique. We also noted there was a need for 3 additions to the NIST catalog as either an aspect of a current control or an entirely new control:

- SC-XX Phone only Mode–Control to specify a requirement for implementing a mode whereby only the use of the mobile device phone service is available.
- AC-XX Events Driven Access Control–Dynamic access control changes based on environmental context as perceived by the mobile device's suite of sensors.
- SC-XY Multiple Independent Security Domains–Specifies the requirement to implement multiple independent security domains in support of personalities, as well as how these domains would provide an information flow and how the information assertions would be implemented on the device via a universally trusted service such as a reference monitor.

3. Proposed Approach

Using our mobile unique controls as a guide, we developed several approaches to mobile manage device information flow including:

- Decentralized Information Flow–Each COI defines the personality information flow enforcement independently from all other COIs
- Centralized Information Flow–A dominate COI is selected which ensures its related personality has preference over all other personalities and either sets a precedence for all personalities or allows the user to resolve all conflict among all other personalities

4. Analysis and Conflict Identification

We found that the decentralized approaches allow for conflicts between the information flow enforcement of personalities. These conflicts occur when the security policies among two or more COIs overlap, especially regarding sensors. Since these COI security policies are non-comparable, no one policy takes precedence over another. This has the potential of leading to a security policy violation for one or more of the COIs which have the overlap. These conflicts are not easily resolved. The user could resolve the conflicts, but this would either defeat MAC access enforcement, sacrifice confidentiality, or sacrifice availability. Also in this approach, the user may not have the requisite information to make such policy decisions.

We found in the centralized approaches, the same conflicts could also occur. Only, as the personality providing the over-all information flow management, the DoD, for instance, would ensure its personality is dominant. This solves the problem for DoD, but this approach may still violate overlapping information flow enforcement of the other personalities. This occurs unless the number of personalities is limited to the user and the one centralized organization or an unlikely agreement is reached among the COIs.

There are certainly many other approaches to mobile device security. We described a number of ways in which mobile devices may be used in the future. We hope to have identified ways in which we can prepare now to meet those challenges. In the end, we perceive more conflicts between the use of the device and the information flow enforcement required by the different stakeholders, specifically the DoD. Such conflicts will have identified and addressed.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] C. Heininger. (2011, April 18). *Army develops smartphone framework, applications for the frontline* [Online]. Available: http://www.army.mil/article/55096/army-develops-smartphone-framework-applications-for-the-front-lines/

[2] Raytheon. (2011, May 20). S*ystem runs on android mobile operating system*" [Online]. Available: http://www.raytheon.com/newsroom/technology/rtn09_rats/index.html.

[3] Electronista. (2012, March 23). *Army software marketplace now live for iOS, Android soon* [Online]. Available: http://www.electronista.com/articles/12/03/23/army.switches.on.custom.mobile.app.store/.

[4] *Guidelines for Managing and Securing Mobile Devices in the Enterprise,* NIST SP 800–124, 2012.

[5] Goodwill Community Foundation, Inc. (2012, April). *GCFLearnFree.org* [Online]. Available: http://www.gcflearnfree.org/computerbasics/9

[6] Android Open Source Project (AOSP). (2011, August). *About the android open source project* [Online]. Available: http://source.android.com/about/index.html

[7] J. Vega and B. Michael, "Mobile device security," *IEEE Security and Privacy,* pp. 11–12, March 2010.

[8] K. W. Miller, J. Voas, and G. F. Hurlburt, "BYOD: security and privacy considerations," *IEEE IT Professional,* vol. 14, no. 5, p. 3, Oct 2012.

[9] Fitbit. (2013, March). *Compare devices* [Online]. Available: http://www.fitbit.com/comparison/trackers

[10] K. Franco. (2012, January 5). *New 7-Day body monitor patch from BodyMedia & Avery Dennison Medical Solutions will aid in wellness initiatives* [Online]. Available: http://vancive.averydennison.com/en/home/newsroom/press-releases/body-media-metria-press-release-010512.html

[11] R. Needleman. (2012, July 13). *Unbreakable: Mesh networks are in your smartphone's future* [Online]. Available: http://www.cnet.com/8301–30976_1–57471447–10348864/unbreakable-mesh-networks-are-in-your-smartphones-future/

[12] *Information Assurance (IA) Implementation,* DoDI 8500.2, 2003.

[13] *Security and Privacy Controls for Federal Information Systems and Organizations Revision 3,* NIST SP 800–53, 2009.

[14] F. Cuadrado and J. C. Dueñas, "Mobile application stores: success factors, existing approaches, and future developments," *IEEE Communications Magazine,* p. 7, November 2012.

[15] Square. (2013, March). *Anyone can accept credit cards with square* [Online]. Available: https://squareup.com/register#anyone-can-accept

[16] M. Swan, "Sensor mania! The Internet of things, wearable computing, objective metrics, and the quantified self 2.0," *Journal of Sensor and Actuator Networks,* pp. 217–253, 8 November 2012.

[17] S. Mann. (2012, December). *The encyclopedia of human-computer interaction, 2nd Ed* [Online]. Available: http://www.interaction-design.org/encyclopedia/wearable_computing.html

[18] K. S. Perez and J. A. Tardif, "Event augmentation with real-time information," U.S., 20 May 2011.

[19] S. Shankland. (2012, June 27). *Google Glass explorer edition* [Online]. Available: http://reviews.cnet.com/camcorders/google-glass-explorer-edition/4505–9340_7–35339166.html?ttag=fbwp

[20] D. Forbes. (2012, November 01). *Best inventions of the Year 2012* [Online]. Available: http://techland.time.com/2012/11/01/best-inventions-of-the-year-2012/slide/google-glass/

[21] Technoz. (2013, February 22). *Google glass: future* [Online]. Available: http://technoz.net/google-glass-future/

[22] D. Goldman. (2012, April 4). *Google unveils 'Project Glass' virtual-reality glasses* [Online]. Available: http://money.cnn.com/2012/04/04/technology/google-project-glass/?source=cnn_bin. [Accessed 17 December 2012].

[23] *Google. (2013, March). What it does* [Online]. Available: http://www.google.com/glass/start/what-it-does/

[24] H. Degans. (2012, December 5). *Imec and UGent unveil breakthrough in augmented reality contact lens - Curved LCD display holds widespread potential for medical and cosmetic applications* [Online]. Available: http://www2.imec.be/be_en/press/imec-news/imecugentcontactlensdisplay.html

[25] B. Hodill. (2012, November29). *Scanadu unveils family of new tools to revolutionize consumer healthcare* [Online]. Available: http://www.scanadu.com/news/

[26] TechNewsDaily. (2011, August 23). *Antenna clothing adds convenience for burdened army grunts* [Online]. Available: http://www.technewsdaily.com/5188-antenna-clothing-soldiers-fashion.html.

[27] M. Bishop, *Computer Security: Art and Science*, Upper Saddle River: Pearson Educational, Inc., 2002.

[28] H. Nissenbaum, “Where computer security meets national security,” *Ethics and Information Technology,* pp. 61–73, 1 July 2005.

[29] D. F. Sterne, “On the buzzword `security policy,’” *1991 IEEE Computer Society Symposium on Research in Security and Privacy*, Gleenwood, 1991.

[30] G. W. Dinolt, *Security Policies,* Naval Postgaduate School, 2009.

[31] *Information Assurance (IA),* DoDD 8500.01E*,* 2007.

[32] DISA (FSO). (2013, March). *STIGs* [Online]. Available: http://iase.disa.mil/stigs/

[33] *Security and Privacy Controls for Federal Information Systems and Organizations Revision 4 Final Public Draft,* NIST SP 800–53, 2013.

[34] *Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.0*, NIST SP 800–117*,* 2010.

[35] *Guide for Applying the Risk Management Framework to Federal Information Systems,* NIST SP 800–37, 2010.

[36] *National Checklist Program for IT Products - Guidelines for Checklist Users and Developers*, NIST SP 800–70, 2011.

[37] *Guide for Mapping Types of Information and Information Systems to Security Categories*, NIST SP 800–60, 2008.

[38] *Standards for Security Categorization of Federal Information and Information*, *FIPS PUB 199*, 2004.

[39] *Minimum Security Requirements for Federal Information and Information Systems*, FIPS PUB 200, 2006.

[40] NIST. (2012, May 16). *Risk Management Framework (RMF) overview* [Online]. Available: http://csrc.nist.gov/groups/SMA/fisma/framework.html

[41] *Classified National Security Information,* Executive Order 13292, 2003.

[42] *Access to Classified Information,* Executive Order 12968*,* 1995.

[43] *DoD Information Security Program*, DoDI 5200.01*,* 1992.

[44] S. Harris, *All In One CISSP Exam Guide*, New York: McGraw-Hill, 2008.

[45] *Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII)*, 2006.

[46] *Protection of Sensitive Department of Defense (DoD) Data at Rest On Portable Computing Devices*, 2006.

[47] *Reducing Risk of Removable Media in National Security Systems (NSS)*, CNSSAM IA 1–10, 2010.

[48] *CNSSI-1253: Security Categorization and Control Selection for National Security Systems,* CNSSI-1253, 2012.

[49] *Communications Security (COMSEC) Utility Program*, CNSSI-4007, 2007.

[50] *Guidelines for Voice Over Internet Protocol (VOIP) Computer Telephony*, CNSSI-5000, 2007.

[51] *National Information Assurance Instruction for Computerized Telephone Systems*, CNSSI-5002, 2012.

[52] *National Policy for Safeguarding and Control of COMSEC Material,* CNSSP-1*,* 2004.

[53] *National Policy Governing the Release of IA products/Services to Authorized U.S. Persons or Activities that are Not a Part of the Federal Government, CNSSP-14,* 2002.

[54] *National Information Assurance Policy on Wireless Capabilities, CNSSP-17,* 2010.

[55] *National Policy for Public-Key Infrastructure (PKI) in NSS,* CNSSP-25*,* 2009.

[56] Common Criteria. (2013, March 17). *Common Criteria* [Online]. Available: http://www.commoncriteriaportal.org/cc/

[57] *Acquiring Commercially Available Software*, DoD CIO Guidance and Policy Memorandum No. 12–8430, 2000.

[58] *Interoperability and Supportability of IT and NSS*, DoDD 4630.05, 2007.

[59] *Use of Commercial Wireless Devices, Services, and Tech in the DoD GIG*, DoDD 8100.02, 2007.

[60] *Protection of Mission Critical Functions to Achieve Trusted Systems*, DoDI 5200.44, 2012.

[61] *Commercial Wireless Local Area Network (WLAN) Devices, Systems, and Technologies*, DoDI 8420.01, 2009.

[62] *Communication Security (COMSEC)*, DoDI 8523.01, 2008

[63] *Use of Mobile Code Technologies in DoD Information Systems*, DoDI 8552.01, 2006.

[64] *The next generation of Common Access Card (CAC) Implementation Guidance*, DoD USD DTM-08–003, 2012.

[65] *Controlled Unclassified Information*, Executive Order 13556, 2010.

[66] *Security Requirements for Cryptographic Modules*, FIPS PUB 140–2, 2001.

[67] *Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, M-05–24, 2005.

[68] *National COMSEC Instruction Protection of Government Contractor Telecoms,* NACSI-6002*,* 1984.

[69] *National Policy on Security Voice Communications,* NSTISSP-101*,* 1999.

[70] *Computer Security Incident Handling Guide,* NIST SP 800–61 Revision 2*,* August, 2012.

[71] *Guidelines for Securing Wireless Local Area networks,* NIST SP 800–153*,* 2012.

[72] P. Kapustka. (2012, July 18). *Voice over LTE explained: better voice quality coming soon to your 4G phone* [Online]. Available: http://www.pcworld.com/article/259471/voice_over_lte_explained_better_voice_quality_coming_soon_to_your_4g_phone.html

[73] J. Serbu. (2013, February 27). *DoD's new plan promises speedy approval of commercial mobile devices* [Online]. Available: http://www.federalnewsradio.com/405/3235070/DoDs-new-plan-promises-speedy-approval-of-commercial-mobile-devices

[74] *Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), NIST SP 800–164,* 2012.

[75] Foursquare. (2013, March 11). *About foursquare* [Online]. Available: https://foursquare.com/about/.

[76] Facebook. (2013, March 11). *Facebook* [Online]. Available: https://www.facebook.com/facebook/info

[77] J. P. Anderson, "Computer security technology planning study," Air Force Electronic Systems Division, Hanscom AFB, Bedford, MA, 1972.

[78] DISA, "Mobile Operating System (OS) security requirements guide V1 R1," 2012.

[79] DISA, "Mobile Device Manager (MDM) security requirements guide V1R1," 2013.

[80] DISA, “Mobile application security requirements guide,” 2012.

[81] DISA, “Mobile policy security requirements guide V1 R1,” 2013.

[82] DISA, “General mobile device (Non-Enterprise activated) STIG V1 R1,” 2012.

[83] NSA, “Mobility capability package,” 2012.

[84] *DoD Information Security Program and Protection of Sensitive Compartmented,* DoDI 5200.01*,* 2008.

[85] Google. (2013, March 11). *Permissions* [Online]. Available: http://developer.android.com/guide/topics/security/permissions.html#broadcasts

[86] P. A. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, “Android permissions: user attention, comprehension, and behavior,” in *Symposium on Usable Privacy and Security (SOUPS)*, Berkeley, 2012.

[87] NSA, “NSA/CSS storage device declassification manual*,”* 2000.

[88] *Guidelines for Media Sanitization,* NIST SP 800–88*,* 2006.

[89] D. Amrit, “An algorithm for Secure formatting of memory,” *International Journal of Computers & Distributed systems,* 1 August 2012.

[90] B. Lee, K. Son, D. Won, and S. Kim, “Secure data deletion for USB flash memory,” *Journal of Information Science and Engineering,* pp. 933–952, 2011.

[91] G. Pecherle, C. Gyorodi, R. Gyorodi, B. Andronic, and I. Ignat, “New method of detection and wiping of sensitive information,” pp. 145–148, 2011.

[92] S. Subha, “An algorithm for secure deletion in flash memories,” pp. 260–262, 2009.

[93] X. Wang, G. Dong, L. Pan, and R. Zhou, “Error correction codes and signal processing in flash memory,” pp. 57–82, 2010.

[94] R. A. Baratto, S. Potter, G. Su, and J. Nieh, “MobiDesk: mobile virtual desktop computing,” in *Annual International Conference on Mobile Computing and Networking (MobiCom ‘04)*, New York, 2004.

[95] K. Nimura, H. Ito, Y. Nakamura, and K. Yasaki, “A secure use of mobile applications with cloud services,” 2010.

[96] H. Wen, Y.-R. P. Huang, A. Archinal, and J. Fagan, “Countermeasures for GPS signal spoofing,” *ION GNSS,* pp. 13–16, 2005.

[97] J. Smith. (2013, February 21). *iPhone 5S: apple’s newest patents tell us ‘S’ is for security [*Online]. Available: http://www.gottabemobile.com/2013/02/21/iphone-5s-apples-newest-patents-tell-us-s-is-for-security/?gbmsl=4

[98] G. H. Software. (2013, March 11). *Green Hills platform for trusted mobile devices* [Online]. Available: http://www.ghs.com/products/mobile_devices.html.

[99] C. L. Nerup, “A high assurance framework for mobile/wireless device Applications,” Open Kernel Labs, 2012.

[100] M. Konstant. (2012, February 27). *Open kernel labs and LG developing “Defense-Grade” mobile devices* [Online]. Available: http://www.ok-labs.com/releases/release/ok-labs-and-lg-developing-defense-grade-mobile-devices/

[101] R. B. Software. (2013, March 11). *vLogix mobile for mobile virtualization”* [Online]. Available: http://www.redbend.com/en/products-solutions/mobile-virtualization/vlogix-mobile-for-mobile-vitrualization

[102] X. Zhang, O. Acicmez, and J.-P. Seifert, *A Trused Mobile Phone reference Architecture via Secure Kernel,* Alexandria, Virginia: ACM, 2007.

[103] Samsung. (2013, February 28). *VMware Mobile Virtualization Platform* [Online]. Available: http://www.samsung.com/global/business/mobile/solution/virtualization/vmware-mobile-virtualization-platform.

[104] T. M. Takai, “Department of Defense mobile device strategy,” Department of Defense, Washington, DC, 2012.

[105] J. Edwards. (2012, April 3). *Tactical radios and mobile devices: Powered by imagination* [Online]. Available: http://defensesystems.com/Articles/2012/03/28/Cover-Story-tactical-radios-mobile-devices.aspx?Page=1

[106] PCMAG.COM. (2012, December 17). *The computer language company Inc.* [Online]. Available: http://www.pcmag.com/encyclopedia_term/0,2542,t=tablet+computer&i=52520,00.asp

[107] C. Ngak. (2013, February 20). *Google Glass preview gives glimpse of how it "feels"* [Online]. Available: http://www.cbsnews.com/8301–205_162–57570302/google-glass-preview-gives-glimpse-of-how-it-feels/

[108] Trusted Computing Group (TCG), "TCG mobile reference architecture," Trusted Computing Group, 2007.

[109] J. Winter, "Trusted mobile platforms," Institute for Applied Information Processing and Communcations (IAIK), Graz university of Technology, 2012.

[110] Open Handset Alliance. (2012, Janary 3). *Open handset alliance* [Online]. Available: http://www.openhandsetalliance.com.

[111] M. Weir, L. M. Gruppe, F. E. Spade, and S. Swanson, *Reliably erasing data from flash-based solid state drives,* 2010.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Jeffrey Bullock
   Space and Naval Warfare Systems Center Atlantic
   Charleston, SC

4. David Carroll
   Department of Homeland Security
   Washington, DC

5. Bruce Carter
   Space and Naval Warfare Systems Center Atlantic
   Charleston, SC

6. Kevin Cox
   United States Department of Justice
   Washington, DC

7. John Christensen
   Space and Naval Warfare Systems Center Atlantic
   Charleston, SC

8. Dr. George Dinolt
   Naval Postgraduate School
   Monterrey, CA

9. Capt. Joshua Dixon
   Marine Corps Systems Command
   Quantico, VA

10. Dr. Al Emondi
    Space and Naval Warfare Systems Center Atlantic
    Charleston, SC

11. Erick Fry
Space and Naval Warfare Systems Center Atlantic
Charleston, SC

12. Cristina Gillaspie
Space and Naval Warfare Systems Center Atlantic
Charleston, SC

13. Jeff Grover
Department of the Army
Aberdeen Proving Ground, MD

14. Jennifer Guild
Naval Sea Systems Command
Keyport, WA

15. Dwayne Higgins
Space and Naval Warfare Systems Center Atlantic
Charleston, SC

16. David Johnson
Space and Naval Warfare Systems Center Atlantic
Charleston, SC

17. Dale Koeman
Space and Naval Warfare Systems Center Atlantic
Charleston, SC

18. Wayne Lathrop
Space and Naval Warfare Systems Center Atlantic
Charleston, SC

19. John Loucades
National Security Agency
Ft. Meade, MD

20. Dr. Peter Majumdar
Marine Corps Systems Command
Quantico, VA

21. Capt. Joe McCaffrey
Information Assurance Directorate at NSA
Ft. Meade, MD

22. John Mildner
Space and Naval Warfare Systems Center Atlantic
Charleston, SC

23. Dr. Ron Ross
National Institute of Standards (NIST)
Gaithersburg, MD

24. Damon W. Shivvers
Space and Naval Warfare Systems Center Atlantic
Charleston, SC

25. Michael Stapleton
Space and Naval Warfare Systems Center Atlantic
Charleston, SC

26. Anthony Soules
Booz Allen Hamilton
Quantico,VA

27. Peter Ward
Space and Naval Warfare Systems Center Atlantic
Charleston, SC